IMPLEMENTATION OF THE COMPUTER SECURITY ACT

HEARING

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION,
AVIATION AND MATERIALS

AND THE

SUBCOMMITTEE ON
SCIENCE, RESEARCH AND TECHNOLOGY

OF THE

COMMITTEE ON
SCIENCE, SPACE, AND TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED FIRST CONGRESS

FIRST SESSION

MARCH 21, 1989

[No. 18]

Printed for the use of the
Committee on Science, Space, and Technology

U.S. GOVERNMENT PRINTING OFFICE
98-075 ⇐ WASHINGTON : 1989

For sale by the Superintendent of Documents, Congressional Sales Office
U.S. Government Printing Office, Washington, DC 20402

H701-64

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

ROBERT A. ROE, New Jersey, *Chairman*

GEORGE E. BROWN, Jr., California
JAMES H. SCHEUER, New York
MARILYN LLOYD, Tennessee
DOUG WALGREN, Pennsylvania
DAN GLICKMAN, Kansas
HAROLD L. VOLKMER, Missouri
HOWARD WOLPE, Michigan
BILL NELSON, Florida
RALPH M. HALL, Texas
DAVE McCURDY, Oklahoma
NORMAN Y. MINETA, California
TIM VALENTINE, North Carolina
ROBERT G. TORRICELLI, New Jersey
RICK BOUCHER, Virginia
TERRY L. BRUCE, Illinois
RICHARD H. STALLINGS, Idaho
JAMES A. TRAFICANT, Jr., Ohio
LEE H. HAMILTON, Indiana
HENRY J. NOWAK, New York
CARL C. PERKINS, Kentucky
TOM McMILLEN, Maryland
DAVID E. PRICE, North Carolina
DAVID R. NAGLE, Iowa
JIMMY HAYES, Louisiana
DAVID E. SKAGGS, Colorado
JERRY F. COSTELLO, Illinois
HARRY JOHNSTON, Florida
JOHN TANNER, Tennessee
GLEN BROWDER, Alabama

ROBERT S. WALKER, Pennsylvania*
F. JAMES SENSENBRENNER, Jr., Wisconsin
CLAUDINE SCHNEIDER, Rhode Island
SHERWOOD L. BOEHLERT, New York
TOM LEWIS, Florida
DON RITTER, Pennsylvania
SID MORRISON, Washington
RON PACKARD, California
ROBERT C. SMITH, New Hampshire
PAUL B. HENRY, Michigan
HARRIS W. FAWELL, Illinois
D. FRENCH SLAUGHTER, Jr., Virginia
LAMAR SMITH, Texas
JACK BUECHNER, Missouri
CONSTANCE A. MORELLA, Maryland
CHRISTOPHER SHAYS, Connecticut
DANA ROHRABACHER, California
STEVEN H. SCHIFF, New Mexico
TOM CAMPBELL, California

Harold P. Hanson, *Executive Director*
Robert C. Ketcham, *General Counsel*
Carolyn C. Greenfeld, *Chief Clerk*
David D. Clement, *Republican Chief of Staff*

Subcommittee on Transportation, Aviation and Materials

TIM VALENTINE, North Carolina, *Chairman*

DAN GLICKMAN, Kansas
DAVE McCURDY, Oklahoma
BILL NELSON, Florida
TOM McMILLEN, Maryland
GEORGE E. BROWN, Jr., California
(Vacancy)

TOM LEWIS, Florida
CHRISTOPHER SHAYS, Connecticut
DANA ROHRABACHER, California
TOM CAMPBELL, California

Subcommittee on Science, Research and Technology

DOUG WALGREN, Pennsylvania, *Chairman*

GEORGE E. BROWN, Jr., California
HOWARD WOLPE, Michigan
LEE H. HAMILTON, Indiana
DAVID E. PRICE, North Carolina
NORMAN Y. MINETA, California
TERRY L. BRUCE, Illinois
DAVID R. NAGLE, Iowa
DAVID E. SKAGGS, Colorado
JERRY F. COSTELLO, Illinois
HARRY JOHNSTON, Florida
JIMMY HAYES, Louisiana
GLEN BROWDER, Alabama

SHERWOOD L. BOEHLERT, New York
CLAUDINE SCHNEIDER, Rhode Island
DON RITTER, Pennsylvania
PAUL B. HENRY, Michigan
CONSTANCE A. MORELLA, Maryland
TOM CAMPBELL, California
D. FRENCH SLAUGHTER, Jr., Virginia
JACK BUECHNER, Missouri

---

*Ranking Republican Member.

CONTENTS

WITNESSES

Page

March 21, 1989:
- Jay Plager, Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget 2
- Raymond G. Kammer, Acting Director, National Institute of Standards and Technology, accompanied by James Burrows, Director, National Computer Systems Laboratory 21
- VADM W. O. Studeman, U.S. Navy, Director, National Security Agency; accompanied by Dr. James J. Hearn, Deputy Director for Information Security, and Patrick R. Gallagher, Jr., Director, National Computer Security Center 72
- Curtis J. Smith, Associate Director For Career Entry and Employee Development, Office of Personnel Management 95
- Francis A. McDonough, Deputy Commissioner For Federal Information Resources Management, General Services Administration 106
- Howard G. Rhile, Jr., Associate Director, Information Management and Technology Division, General Accounting Office, accompanied by David Gill 117

IMPLEMENTATION OF THE COMPUTER SECURITY ACT

TUESDAY, MARCH 21, 1989

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND
MATERIALS, AND SUBCOMMITTEE ON SCIENCE, RESEARCH AND
TECHNOLOGY,
Washington, D. C.

The subcommittees met at 2:05 p.m. in Room 2318 of the Rayburn House Office Building, the Honorable Tim Valentine and the Honorable Doug Walgren, chairmen of the subcommittees, presiding.

Present: Representatives Valentine, Walgren, Lewis, Henry, Glickman, Morella, Rohrabacher, McMillen, Buechner and Campbell.

[2:05 p.m.]

Mr. VALENTINE (Presiding): We'll get started. Maybe we'll be joined by more members as time goes on.

The Subcommittee on Transportation, Aviation and Materials meets today for an Oversight Hearing on Computer Security. We are pleased to be meeting with our colleagues from the Science, Research and Technology Subcommittee, whose Chairman at least will join us later to review the progress by federal agencies in implementing the Computer Security Act of 1987.

The Act, which originated in this Subcommittee, will, when fully implemented, achieve a major improvement in a potentially very serious national problem, namely, the security and privacy of information held in government computers.

Virtually every agency in the federal government, along with thousands of other organizations that carry out tasks on behalf of the government, is highly dependent on the use of computers. And computers, as we have seen over and over again, are vulnerable to all manner of improper actions.

The Computer Security Act was passed to raise the awareness of the vulnerabilities and to require agencies to take steps to protect the information in their computers.

Specifically, each agency was required by the Act to develop and submit on January 8th a security plan for each of its computer systems.

Our purpose today is to review the progress being made in achieving this milestone, as well as to oversee efforts by the lead agencies, that is, OMB, NIST, NSA, GSA and OPM, in implementing other important features of the Act.

Each of the organizations represented here today has been working very hard to make the Act successful. And I would like to thank for both of these Subcommittees and all of the members, I would like to thank each of them.

I would like especially to acknowledge publicly the efforts of the Office of Management and Budget. Without OMB's leadership, it would be impossible to make progress in the complex task of improving computer security.

I recognize at this time the Ranking Republican Member of the Subcommittee, my good friend, Tom Lewis.

Mr. **Lewis**. Thank you, Mr. Chairman.

The March 3, 1989 Public Announcement of the Computer Spy Ring stated that a West German citizen worked for two years to gain access to more than 30 computers, including those of DoD, NASA and DOE.

While no secret military information was taken, sensitive data was possibly given to Soviet agents. The Computer Security Act addresses this type of information. I look forward to hearing today's witnesses address this and other computer security problems, Mr. Chairman.

The Computer Security Act had a controversial path, especially in defining the duties of NSA and NIST. Both agencies appear to be working out their differences successfully.

Thank you, Mr. Chairman.

Mr. **Valentine**. Thank you.

I recognize Congressman Paul Henry.

Do you have any opening statement? We'll be glad to hear from you, sir.

Mr. **Henry**. I just commend you, Mr. Chairman, for renewing the hearings you began last fall on this Act.

Thank you.

Mr. **Valentine**. Thank you, sir.

Our first witness is Mr. Jay Plager, Administrator of the Office of Information and Regulatory Affairs for the Office of Management and Budget. We're glad to have you here, sir. Your prepared statement will appear in the record in toto. Feel free to summarize or proceed in any other way that you deem appropriate.

STATEMENT OF MR. JAY PLAGER, ADMINISTRATOR, OFFICE OF INFORMATION AND REGULATORY AFFAIRS, OFFICE OF MANAGEMENT AND BUDGET

Mr. **Plager**. Thank you very much, Mr. Chairman. I appreciate very much your receiving my prepared statement. If I may, I'd like to make a few brief comments on where we are, then I'll be glad to answer any questions that you or other members of the Committee may have.

I appreciate the opportunity to describe the Office of Management and Budget's continuing efforts to implement the Computer Security Act of 1987. As I testified last September, OMB has long had an interest in the security of federal automated information systems.

In this fiscal year, the federal government will invest $17 billion in its information technology systems. While that investment is large, its impact on the business of government is even larger. It is hard to imagine a significant government program today that is not critically dependent on computers to operate effectively.

Since "security" means basically assuring that federal computer systems do exactly what they are supposed to do and nothing more, adequate security of the computers that support federal programs is essential to the proper functioning of the programs and, thus, to the federal government itself.

When I was here in September, we were nine months into the first year of implementing the Computer Security Act. The federal agencies were developing security plans for their computer systems that contained sensitive information. To assist them, OMB had issued guidance in the form of OMB Bulletin 88-16.

At the same time, the agencies were implementing computer security awareness and training programs consistent with OPM's July 1988 regulation.

At the September hearing, I described our activities to date in implementing the Computer Security Act and I said I thought that the agencies had made a good start toward implementing the Act.

I also said that we would continue these efforts to improve the security of federal computer systems.

The Subcommittee asked about the continued implementation of the Act and particularly the relationship between the National Institute of Standards and Technology and the National Security Agency under the Act.

I am pleased to be able to report that, since September, we have made considerable progress toward assuring effective implementation of the Act. The 1990 President's budget proposes doubling the budget for NIST's computer security activities.

In October, NIST and NSA co-sponsored a two-day workshop to discuss agency computer security planning efforts, answer questions agency staff had concerning the planning guidance in OMB Bulletin 88-16 and to discuss agency computer security awareness and training programs.

In accordance with the Computer Security Act, the agencies have begun submitting their plans for the security of computer systems that contain sensitive information to a Joint NIST/NSA Review Team for advice and comment.

As of last week, 60 agencies had submitted more than 1,500 plans, including some plans from all of the largest agencies, although many of the largest of those agencies have not yet completed submission of all of their plans.

NIST working with OPM has issued computer security awareness and training guidelines for federal agencies and contractors as required by the Act.

Earlier this month, the inaugural meeting of the Computer System Security and Privacy Advisory Board was held. NIST and NSA have reached agreement on a Memorandum of Understanding that formalizes their working relationship in computer security.

At the same time that we have been making progress in implementing the Computer Security Act, new evidence of federal computer vulnerabilities have surfaced, illustrating the wisdom of having a governmentwide program for computer security.

As we all remember, back in November, a computer virus was introduced into the ARPANET computer network. I should note that we called it a virus, but I am told by the people who really know that it is a worm. But, I'll call it a virus because I think people have used that term more often.

This virus was introduced into the network with serious, although fortunately not fatal, consequences. Such attacks represent a growing threat to our networks of computer systems.

As a result, in December, we asked the Secretaries of Commerce and Defense, the Attorney General and the Administrator of General Services to participate with us in assessing the nature and magnitude that this relatively new threat represents to federal systems.

That review is to be completed later this spring.

In October, the President's Council on Integrity and Efficiency reported that its staff was able to penetrate 10 of the largest federal computer centers through use of a common known vulnerability in those systems. In November, we notified agency heads of this report's findings and asked that they take action in line with the report's recommendations.

We not only asked them to correct the control weaknesses specifically identified in the report, but more importantly suggested that they use the computer security planning activity already in progress in accordance with the Computer Security Act as a way to assure that their other computer systems did not have similar weaknesses.

Mr. Chairman, we are continuing our efforts to implement the Computer Security Act of 1987. We believe the Act gives us a framework and provides the momentum for the government to address the security of federal computer systems, and we believe that the agencies have made a good start.

We believe that our computer systems are more secure today as a result of the Act and the actions taken pursuant to the Act than they were last January. But, obviously, much still remains to be done.

The work and interest of this Committee, as well as the House Government Operations Committee and the GAO, have been important factors in assuring a high-level of attention to this vital activity.

We look forward to continuing to work closely with the Committee on this effort. I'd be pleased to answer any questions that you or other members of the Committee may have.

[The prepared statement of Mr. Plager follows:]

Insert T-1

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

STATEMENT OF JAY PLAGER
ADMINISTRATOR
OFFICE OF INFORMATION AND REGULATORY AFFAIRS
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE SUBCOMMITTEES ON
TRANSPORTATION, AVIATION AND MATERIALS
AND SCIENCE, RESEARCH AND TECHNOLOGY
OF THE COMMITTEE ON SCIENCE, SPACE AND TECHNOLOGY
OF THE HOUSE OF REPRESENTATIVES OF THE UNITED STATES
ON IMPLEMENTATION OF THE COMPUTER SECURITY ACT OF 1987
MARCH 21, 1989

Mr. Chairman and Members of the Subcommittees:

I appreciate the opportunity to describe the Office of Management and Budget's (OMB's) continuing efforts to implement the Computer Security Act of 1987 (P.L. 100-235).

As I testified last September, OMB has long had an interest in the security of Federal automated information systems. In this fiscal year the Federal government will invest $17 billion in its information technology systems. While that investment is large, its impact on the business of government is enormous. Every government program is critically dependent on computers to operate effectively, including the Federal programs that distribute benefits, collect revenues, assure public safety, and defend our nation. Adequate security of the computers that support those programs, (i.e. assuring that they do exactly what they are supposed to do and nothing more), is essential to the proper functioning of the programs themselves and to the Federal government.

When I was here in September, we were nine months into the first year of implementating the Computer Security Act of 1987. The Federal agencies were developing security plans for their computer systems that contain sensitive information. To assist them, we had issued OMB Bulletin 88-16, "Guidance for the Preparation and Submission of Security Plans for Federal Computer Systems Containing Sensitive Information." At the same time, the agencies were implementing computer security awareness and training programs consistent with OPM's July 1988 regulation. At that hearing I described our activities to date in implementing the Computer Security Act and I said that I thought that the agencies had made a good start toward implementing the Act. I also said that we would continue these efforts to improve the security of Federal computer systems. The Subcommittee expressed interest in the continued implementation of the Act, and asked about the relationship between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) under the Act.

Implementation Activities

Since September, we have continued to work with the other key agencies to assure effective implementation of P.L. 100-235:

- The 1990 President's budget proposes doubling the budget for NIST's computer security activities.

- In October, NIST and NSA co-sponsored a two day workshop to discuss agency computer security planning efforts, answer questions agency staff had concerning the planning guidance in OMB Bulletin 88-16, and to discuss agency computer security awareness and training programs.

- In accordance with the Computer Security Act, agencies have begun submitting their plans for the security of computer systems that contain sensitive information to a joint NIST/NSA review team for advice and comment. As of March 13, 1989, 60 agencies have submitted more than 1500 plans, including some plans from all of the largest agencies, although many of the largest of those agencies have not yet completed submission of their plans.

- NIST, working with OPM, has issued computer security awareness and training guidelines for Federal agencies and contractors as required by the Act.

- Earlier this month, the inaugural meeting of the Computer System Security and Privacy Advisory Board was held.

- Last week NIST and NSA reached agreement in principle on formalizing their working relationship in computer security.

Recent Security Incidents

At the same time we have been making progress in implementing the Computer Security Act, new evidence of Federal computer vulnerabilities has surfaced that illustrates the wisdom of having a government-wide program for computer security.

- In early November, a computer "virus" was introduced into the ARPANET computer network, and during the ensuing days seriously impacted host computer services on that network.

- The President's Council on Integrity and Efficiency (PCIE) reported that its staff was able to penetrate ten of the largest Federal computer centers through use of a common, known vulnerability in those systems.

Computer "Viruses"

Our discussion of computer viruses in September was timely. Less than two months later, the Federal government's largest research network was used to propagate a computer virus attack (the so-called ARPANET virus, although it technically was a "worm") which interrupted service on host computers throughout the United States. Such attacks represent a growing threat to our networks of computer systems. As a result, in December we asked the Departments of Commerce, Defense, the Attorney General, and the Administrator for General Services to participate with us in assessing the nature and magnitude that this relatively new threat represents to Federal systems.

That review, to be completed this Spring, is looking at several broad thrusts for responding to the threat:

1. Short term "fixes," such as an emergency response capability to share information on viruses and assure that technical "vaccines" and "antidotes" are rapidly deployed;

2. Longer term needs, such as initiatives to assure that better preventive mechanisms against viruses are developed; and

3. An assessment of the need for additional Federal legislation, to include an appraisal of the applicability of existing statutory sanctions to virus incidents, and need for further sanctions.

Security Weaknesses Reported by the PCIE

In October, the President's Council on Integrity and Efficiency (PCIE) reported that it found serious control deficiencies in the system software of ten major Federal computer centers. These control deficiencies allowed the PCIE staff to go around many of the security features of those systems and actually penetrate the systems.

In November we notified agency heads of the report's findings and asked that they take action in line with the report's recommendations. We not only asked them to correct the control weaknesses specifically identified in the report, but more importantly suggested that they use the computer security planning activity already in progress in accordance with the Computer Security Act as a way to assure that their other computer systems did not have similar weaknesses.

Computer Security Planning

As I testified in September, we view the submission and review of computer security plans as a process designed to produce better security plans and thus ultimately better security of computer systems. It is not a "gotcha game." For this reason, we have only involved ourselves in that process to assure that agencies are being responsive to the requirements of the Act. In a few instances that involvement called for discussions with agency staff to assure that complete submissions would be sent.

As I noted earlier, NIST and NSA have received more than 1500 plans for review as of March 13, 1989. I will leave it to the NIST and NSA witnesses to discuss the character of those plans in more detail. However, my overall impression is that the agencies have made great progress this first year, particularly in planning for and securing their internal computer systems. At the same time, it appears that some areas of Federal vulnerability may have been overlooked by the agencies. One such area is the security of contractor and grantee (state and local) systems that are run on the government's behalf to accomplish a Federal function. That is clearly an area in which more effort is needed in the future.

But as I said in September, this first year is in part a diagnostic phase, in which we can learn more about where additional guidance may be required. Along that line, later this month, NIST and NSA are co-sponsoring a workshop with the agencies to discuss their experiences in computer security planning thus far. Their input is an important piece of our assessment of the direction of future guidance concerning computer security planning. Certainly, the adequacy of security of contractor and grantee systems will be a topic of discussion with the agencies at that workshop.

The Computer Security Act also recognizes the need to integrate computer security into systems planning and mandates that summaries of computer security plans be included in agency's annual five-year plan required by the Paperwork Reduction Act. This gives us clear direction to integrate the computer security planning process into our general planning and budgeting processes for information technology. This Spring, we will be developing guidance for the agencies to tie these two processes together and thus assure that security planning decisions are integral to basic decisions about information technology systems.

OMB's Computer Security Planning

Your letter specifically asked about the computer security plans for OMB itself. Development of OMB's computer security plans was handled by the Assistant to the Director of OMB for Administration pursuant to his designation as the responsible official under the Paperwork Reduction Act. In our government-wide responsibilities for computer security, OMB is viewed as any other agency, except that I am also responsible for two of OMB's sensitive computer systems, and thus my staff prepared plans for those systems.

As you may know, OMB's computer support is provided by the Office of Administration (OA) within the Executive Office of the President. Thus, our plans consisted of five major application systems, that contained sensitive information consistent with OMB Bulletin 88-16.

In the development of OMB's plans, it became apparent that OMB staff, including my own staff for my applications, had to work jointly with the OA staff to complete the requirements of Bulletin 88-16. The net result was that certain assumptions that each had been making about the security of the systems were discussed and clarified. In the first instance, this process raised the awareness to the security question of OMB users of computer systems. Beyond that, however, there was substantive discussion between the users of computer systems in OMB and the computer center technicians in OA concerning the security risks and needs of those systems -- exactly the communication that we had hoped would occur as part of the planning process.

A joint EOP planning submission was forwarded to NIST/NSA for review last month. To date, we have not received comments on the submission of our plans.

Security Awareness and Training

A key thrust of the Act is that security awareness and training applies not just to computer and computer security professionals, but also to users of systems. Such awareness is essential to improving the security of the systems. After all, it is the users of computer systems, those in the business of running government programs, who must live with the security risk of the systems that support their programs. They must understand how much risk that entails and how they can effectively reduce that risk to an acceptable level.

Passage of the Computer Security Act itself began the process of broadening computer security awareness within the Federal community. Issuance of the Office of Personnel Management's regulation governing security awareness training and security practices for Federal employees in July was the next step. Issuance of NIST's security training guidelines last month should further stimulate this activity as agencies proceed to implement their training programs.

Along that line, we are encouraged by the GAO's findings in its February 1989 report, "Computer Security: Compliance with Training Requirements of the Computer Security Act of 1987". Virtually all of the agencies have taken some action to establish awareness and training programs. Furthermore, most agencies reported that they were satisfied with the OPM regulation and NIST's training guidelines. Most importantly, 62 percent of all reported courses were targeted at end users, including at least one course in virtually all agencies that reported detailed descriptions of their training courses. Apparently that important message in the Computer Security Act is beginning to get out.

Guidelines and Standards

Creating awareness of the security threat and conducting training are not enough. Once awareness is created, viable tools must be available for system managers to tighten the security of their systems. In the short term, we must make the best use of available tools. In the longer term, however, better tools need to be developed. To this end, NIST, drawing upon NSA technical guidelines, is tasked under the Act to develop computer security standards and guidelines. We have proposed substantial funding increases for NIST's activities in this area. It is essential to our implementation of an effective computer security program to have viable tools avaliable when they are asked for by end users.

Coordination of NIST and NSA Activities

Your invitation letter asked that we address the relationship between the computer security and network security programs of the National Security Agency and the National Institute of Standards and Technology. I understand that NIST and NSA recently reached agreement in principle concerning a Memorandum of Understanding on how they will work together on their various responsibilities for Federal computer security. In some ways this agreement is simply a formalization of a developing relationship that has allowed the two agencies to work closely together, for example, in joint review of computer security plans. As you may recall from the September hearings, the primary sticking point was in the development of cryptography standards and guidelines. The memorandum will establish a coordinated review process to address these issues as they arise.

It is essential that these two agencies continue to work closely. To do an effective job, NIST must understand and take maximum advantage of security tools and methodologies developed by NSA when they are applicable. We cannot afford to duplicate unnecessarily the expertise resident at NIST or at NSA. At the same time, the nature of the information each of these agencies is charged to help secure and the potential threats to that information are often very different. The Act acknowledges these differences and provides a rational framework for separate, but cooperative work. For these reasons the two organizations are also actively participating in each other's forums, participation that we encourage and support.

Rewrite of NSDD-145

Your letter also asked that we address the rewrite of NSDD-145. In a recent letter the National Security Advisor asked the Secretary of Defense to draft a replacement for NSDD-145, in coordination with OMB and the Department of Commerce, one that is consistent with the Computer Security Act of 1987.

At the same time, the fact that NSDD-145 has not yet been revised is not impeding implementation of the Computer Security Act. As evidence, the joint review of security plans by NIST and NSA has continued and is working well. Furthermore, the cementing of those agency relationships in the recently agreed to memorandum of understanding between NIST and NSA will temper the urgency to rapidly revise the NSDD.

Conclusion

As I have outlined, we are continuing our efforts to implement the Computer Security Act of 1987. We believe that the Act gives us a framework, and provides the momentum for the government to address the security of Federal computer systems, and we believe that the agencies have made a good start. We believe that our computer systems are more secure today, as a result of the Act, than they were last January. But much still remains to be done. We look forward to continuing to work closely with the Subcommittees on this important effort.

I would be pleased to answer any questions that you may have.

Mr. Valentine. Mr. Plager, are you in the position to give us any suggestions, if, indeed, you have any suggestions, as to whether or not the Act needs any fine- tuning? If it is workable? If you have any ways that you think it could be improved?

I want you to address them here today and let us have your views in writing.

Mr. Plager. All right, sir. I appreciate that very much. I think the Act has been quite workable at this early stage. I think it may be a little bit early to begin the process of fine-tuning. I will assure you that we will keep that issue in mind as we go through the months ahead in dealing with these programs and these plans. And should we find a need for adjustment or improvement of some kind, we will not hesitate to come back to the Committee.

Mr. Valentine. All right, sir. We have been given to understand that certain agencies, such as the Departments of Health and Human Services and Agriculture, did not initially identify the sensitive systems operated on their behalf by States.

Do you believe there should be a degree of assurance that the States are providing computer security for federally-supported programs?

Mr. Plager. The application of the Act to those State and other non-federal computer systems is conditioned in the terms of the Act itself on the need for and appropriateness of computer security needs.

I think that's a sensible way of looking at it. That is to say, some state and other non-federal programs involving federal activities or implicating federal activities may be so clearly sensitive and have such an impact on federal programs that they should be brought fully under the requirements of the Computer Security Act and the processes we are setting in place.

On the other hand, there may be other programs where only a small part of the program activity actually affects or might affect federal activities.

And it seems to us that we should look at this problem in the sense of a continuum, that is, look at it on a range of sensitivities and a range of needs and a range of responses on our part.

That's basically the approach that we're advocating that the system take in dealing with those particular computer systems. In effect, I think what I'm saying is we want insurance and assurance at the same time that the programs that really affect us are secure and the programs that only partly affect us have the security that's appropriate to that degree of effect.

Mr. Valentine. Do you believe also that there should be a degree of assurance as far as the contractors which are providing computer security for federally-supported programs?

Mr. Plager. Yes, sir. I think the same principle applies. The Act is clear that contractors are included, systems held by contractors with the federal government are included. I think the same concern and the same approach is appropriate.

Mr. Valentine. It wouldn't make much sense not to, would it?

Mr. Plager. No, it would not, sir.

Mr. Valentine. The Act calls for annual "updates of the security plans as necessary," quote/unquote. Based on agency responses to date, what type of formal data call do you plan to issue for security plans next year, incorporating NIST and NSA comments?

Mr. PLAGER. I think it's just a little early to describe in any detail what that call should look like, frankly, because we don't honestly know enough yet to be sure what it should look like.

I think we need to get the benefit of this first round of analyses, as I think NSA will testify later this afternoon, and perhaps others. The process calls for a three-stage collection of preliminary analysis and then detailed analysis of each of these plans.

And the first two stages are well along. The third stage is really just beginning by NIST and NSA. When we have the benefits of what those insights give us, I think we'll be in a much better position to decide what the next step needs to be, including what that formal call should look like.

Mr. VALENTINE. Can you tell us how you plan to monitor agencies in order to ensure that they implement their security planning?

Mr. PLAGER. I think that's an excellent question, Mr. Chairman, because it raises a dimension that, at this point, can get lost in the effort we are making to first identify the systems which we've been going through this past fall, then putting the plans in place.

All of that is very important to do. But, ultimately, the real test is:

Do these plans get implemented? Do these systems become more secure both in hardware, software and in the way that users are trained?

I think the emphasis in your question, if I heard it correctly, is on implementation. I think the answer to that is we haven't focused as much on the implementation issue at this stage, simply because it has not yet been the central issue; as we go through the process of identification of systems and then the planning of the program, we are indeed going to move our attention to the implementation process and we have not yet developed full plans for how to do that.

But I think it's a very important step and I'm, frankly, expecting to get considerable help from the Advisory Committee that has already, as I said, had its first meeting, and from the lessons we learn from the NIST/NSA review process.

Mr. VALENTINE. One final question before I yield to my colleagues. As you know, some agencies have responded to the Act by claiming that they have no sensitive systems.

How do you view that? Are they saying that everything they have is in the public domain? Is it possible that an agency of the government has developed data, the loss of which might have no effect on the agency?

If that's the case, maybe we ought to take a look at the agency itself and save some money on the whole operation.

[Laughter.]

Mr. VALENTINE. Would you care to comment on that?

Mr. PLAGER. Earlier, before the hearing started, Mr. Chairman, Mr. Lewis asked me what a Good Gator was doing in OMB. I don't know whether it's my Gator background or my OMB background, but either way, I have some difficulty understanding how there could be a federal agency with absolutely no sensitive systems that was engaged in doing the federal government's work with any effectiveness and efficiency.

So I share the suggestion in your question, and we would look with some question, serious question, on an agency that said they have absolutely no systems that would come within the scope of the Computer Security Act.

I think, if we get such representations, you can be assured that we will ask some very hard questions depending on the circumstances.

Mr. VALENTINE. We hope so. Thank you.

Mr. Lewis.

Mr. LEWIS. Thank you, Mr. Chairman. I guess, Mr. Plager, we should take stock in the fact that you're the first person in years I've heard about here that received some kudos for being from OMB. I think that's great, you know. Put that under your hat.

Mr. PLAGER. All right, sir, I will.

Mr. LEWIS. Are there any estimates for the losses for breaches of security in your agency, or any other agency, that you may be aware of?

Mr. PLAGER. Estimates you mean in terms of cost?

Mr. LEWIS. Cost in dollars or cost in information.

Mr. PLAGER. I do not know of any. None has come before me personally. And as I glance over my shoulder, my senior staff tells me that I do not think we have such data. I'd be glad to go back and ask around. I suspect those data probably simply do not exist because I think we have not been as sensitive to this problem in the past as we should have as a government.

In fact, that is the beauty of the Act and these hearings. And I doubt there was any effort made to gather those data in any collective way.

Mr. LEWIS. It's nice to know there's no worms crawling around the OMB.

What, in your judgment, is the status of the investigation into any of the data breaks that have taken place, taking the data from any of these other agencies?

Are you aware of any other information that has been procured by a worm in some way, that data was removed?

Mr. PLAGER. I really don't know of any. I do not have that information. I do not think it would come to OMB in that form.

I do not wish to put my colleagues on the spot, but perhaps that would be a question that either the NSA or NIST might have more direct information about.

Mr. LEWIS. I'll save that one for them.

How about the Computer Security Act that was passed? Do you feel that this Act can prevent against break-ins, into the computers?

Mr. PLAGER. I think, if the process that that Act has triggered, and if the agencies continue as they have and take this matter as seriously I believe they are now taking it, and if the key agencies—OPM, NSA, NIST and OMB—continue to work as cooperatively as we have, I think the result will be to reduce if not substantially eliminate those risks.

Now, as I mentioned earlier, we can never reduce the risk to zero. For every clever idea we have, there's a lot of folks out there who are trying to be even cleverer, either for games playing or for other reasons. But we can certainly do a lot to reduce that risk and we're working at that.

Mr. **Lewis**. You have gone over the Computer Security Act. Have you seen—does your Department see any excessive costs that would have to be applied in order to provide necessary security under the Act?

Mr. **Plager**. As you might expect, OMB worries about that particular side of the problem. And as I mentioned earlier, we have, in fact, committed substantial additional resources to NIST to assist in its work in this area.

I don't think we view that as excessive. I think we view that as a good investment in an important federal need. And at the present time, our view is that the resources, both direct financial and personnel resources, being put into this are well worth the effort. The benefit cost ratio on this activity is certainly in our favor.

Mr. **Lewis**. Thank you, Mr. Plager.

Thank you, Mr. Chairman.

Mr. **Valentine**. Mr. Glickman.

Mr. **Glickman**. Thank you, Mr. Chairman.

Thank you very much for coming here. I was actually the original prime sponsor of this bill; along with Congressman Brooks, we decided that, frankly, it was precipitated for two reasons.

One was because of the incidence of hackers, publicized hackers back in the early eighties, coupled with the problem of who in our government was responsible for computer security—the National Security Agency or the civilian agencies of government?

That was the prime reason that we moved through this bill. Now, I judge from your testimony that you have no qualms with the legislation. The Administration is totally supportive of the Computer Security Act.

The reason why I asked that is because it was pulling teeth to get the prior Administration to be supportive of this concept. I gather from your testimony that you support it, you intend to do whatever you can to make sure that its implementation is full, complete and expeditious.

Mr. **Plager**. The issue before us now, Mr. Glickman, is not whether the Act should be passed, or whether it should be passed in that form. The issue before us now is that this is a piece of legislation passed by the Congress and approved by the President, and we are implementing it in all good faith and with every effort that we can make.

Yes, sir.

Mr. **Glickman**. The issue sometimes, once a bill is passed, is does the Administration—any Administration—want to do everything within its power to see that it's implemented? Or is it just dragging its feet.

And I just want to know, it is from your mouth as the OMB person in charge of this, that you believe it's a high- priority issue to deal with these issues and do you intend to monitor it and ensure that agencies are in compliance with it?

Mr. **Plager**. That states very correctly our views. We are fully in support and fully working to implement this wholeheartedly.

Mr. GLICKMAN. I don't know if you've seen this article in the Washington Post. It was last month, written by John Burgess. But, in there, they indicate that some folks, including some members of Congress, have been critical of the Administration implementing this as fast as it should be implementing it.

I, myself, have felt that perhaps the implementation of this law is too slow. It has taken a very long time to get agencies to come up with plans and be in compliance with it.

We still have not resolved all of the problems between the National Security Agency and NIST on implementation.

As a member of both this Committee and the Intelligence Committee, I'm aware of some of the problems there. And we also continue to have in existence National Security Directive 145, which is still in place, which was essentially the directive that precipitated the passage of this legislation.

So those things concern me, as somebody whose been involved in this issue.

Specifically with respect to the National Security Directive, which basically gave NSA and DoD fairly extensive powers in dealing with computer security problems involving civilian agencies, what is happening to that directive right now?

You mentioned that, but you're not specific.

Mr. PLAGER. Yes, sir. I don't want to minimize, and I certainly would not to this Committee minimize the complexities and the difficulties in getting everybody to march together to the tune of computer security. It's not something that the agencies naturally came to. It's not something they were doing by and large; some were doing it more than others.

But, you're quite right. It is a slow, arduous process to sort of push and haul and shove everybody along. And we haven't fully succeeded in getting everybody on time.

And as I indicated, we've got 60 agencies with over 1,500 plans already ahead with us. Some of the agencies, as I also indicated in my comments, some of the big agencies have not gotten the plans in for all of their systems. I'm not even sure they've identified all of their systems fully. But they are truly working on it.

You also note the problems we had between NSA and NIST in working on a coordinated approach, and I don't want to minimize that problem either. That took a lot longer than I had hoped it would when I was up here in September.

I assured you that the good offices of OMB and my office were behind the effort to get those two agencies to come to an understanding. And I am pleased to say that that has been accomplished.

I'm less pleased to say how long it took, but it has been done. And agreement has been reached. And I think that document will shortly be signed. And I think, sir, that that lays the groundwork for the solution of the NSDD 145 problem as well.

With regard specifically to NSDD 145, the National Security Advisor has tasked Secretary of Defense to address that issue, and to get it addressed promptly. It is being addressed. Draft documents are already being circulated, and with the MOU between NIST and NSA now in place, or about to be fully in place, I think most of that underbrush has been cleared away.

Mr. GLICKMAN. Do you think there's anything that needs to be done to move the Secretary of Defense, whose being sworn in as I speak to you right now, to move him to accelerate DoD's plans any faster?

After all, they have not been one of the great cooperators in terms of complying with this law.

Mr. PLAGER. I think you just did it, sir.

Mr. GLICKMAN. I did?

Mr. PLAGER. By raising everyone's awareness to your concern and the Committee's concern, I assure you that will be communicated to the Secretary of Defense, and I truly believe that they understand the importance of this and our addressing it.

Mr. GLICKMAN. Let me just conclude by a couple of things. One is I appreciate your testimony and your commitment to this program. If there has ever been an important function of government, it is to protect the information of private citizens contained in computers so that they're safe, that they're not manipulated; whether it's social security information or veterans' information, air traffic control, banking or national security information, computers are the way we store information and contain it and we have to deal with it. It's not an abstract problem, as you can see, with the viruses that are occurring, hackers in West Germany and everything else.

The other thing is this is a program—I never intended this Computer Security Act to be filled with bureaucratese jargon like I've seen. It's almost weighing down the ability of government policymakers to decide all sorts of forms and acronyms.

I know that you are not a person who has spent your whole life working at the highest levels of government. I believe you were the Dean of a law school, right?

Mr. PLAGER. Yes, sir. Ill-prepared for this experience.

[Laughter.]

Mr. GLICKMAN. Well, you're here and you have to do your best with it. I would hope that you would use your lay common sense expertise to know that you have an important function. That function is to make sure that my aunt and the little, old lady who lives down the street can be assured that nobody is going to go into any computers and screw up her social security, or change records in the VA, or make it so that inter-bank transfers are hacked into by some either criminal, or worse, maybe, somebody who could be a terrorist.

It's really important and I guess that would be the point I'd make to you. This is really important stuff that's going on and it tends to get yawns because of the complicated nature of it. And I would just hope that you recognize that.

And I think from your testimony that you appear to do that.

Mr. PLAGER. I share your frustration and also your frustration with the acronyms and the complexity of all the agencies involved. I assure you I share your commitment to the goals you have articulated.

And I can honestly say I've been at OMB now for several years. There is an equal dedication among the professional staff at OMB and in the other agencies, NSA and NIST, to the concerns you expressed.

Mr. GLICKMAN. Thank you, Mr. Chairman.

Mr. **Valentine**. Jay, since you have done so well at this point and been identified as a Floridian and it is now in the record that you are a law school dean, I'd like you to be in a position to confess that you graduated from the University of North Carolina at Chapel Hill.

[Laughter.]

Mr. **Plager**. I did, sir, one of the proudest moments of my life, sir.

[Laughter.]

Mr. **Lewis**. Mr. Chairman, I think it's most important to point out that he graduated from the University of Florida Law School.

Mr. **Valentine**. Anybody else want to get in on this?

[Laughter.]

Mr. **Glickman**. Have you ever been to Kansas?

[Laughter.]

Mr. **Plager**. No, but I'd love to.

[Laughter.]

Mr. **Valentine**. We've got a ticket for you.

Ms. Morella, we're happy to have you here.

Ms. **Morella**. Congressman McMillen and I invite you to Maryland if you've never been there.

Mr. **Plager**. In fact, if I may say, I recently bought a little house down in Maryland near Oxford, and I love your State.

Ms. **Morella**. Very good.

Tom, whose District is that?

Mr. **McMillen**. Roy Dyson's.

Ms. **Morella**. Well, you come through our District on your way here.

I wanted to ask you for your response to an article that was earlier this month I think in the *Washington Post* or *New York Times*. It has to do with West Germans operating a spy ring that violated U.S. computers. I'm wondering how that ties in with how you plan to monitor the agencies to ensure that they implement the security planning.

And what are you doing before the fact and not after the fact to prevent this kind of thing from happening?

Mr. **Plager**. With specific reference to the West German hackers problem, that's one that did get a lot of press attention, and I think one that is getting now a lot of government attention.

The agencies that were involved or were affected by that, it's my understanding, have come together and are looking into that with considerable concern and care.

It's also my understanding that no classified information was compromised by that particular event, although I suppose within the purview of the Computer Security Act, we would say that sensitive information may well be involved.

With regard to the implementation issue, as I mentioned earlier, that's a very important point. And one that is the immediate next set of concerns as we get these plans in effect and the identification of systems in effect.

We then have to, when everybody has gotten a plan that is effective and does the job that the Act called for, we then have to put it in place, the systems, internal monitoring systems, to ensure that we not only have plans but that we actually implement them. And that they actually do what they purport to do.

That is something that OMB is going to be very much concerned and very much involved with, with the other agencies.

Ms. **MORELLA**. In both instances, you cannot answer now but you're looking into both the implementation and what will be done to shore up security to prevent that.

Mr. **PLAGER**. Yes.

Ms. **MORELLA**. Thank you, Mr. Chairman. We'll be looking for the responses.

Mr. **VALENTINE**. Mr. McMillen.

Mr. **MCMILLEN**. Thank you, Mr. Chairman. I was a little overwhelmed to hear that the witness is a Tar Heel, because the Chairman is a tar heel as well.

Mr. **VALENTINE**. He's a man for all seasons and we're being too good to him.

[Laughter.]

Mr. **MCMILLEN**. I appreciate the chance. I have a statement I would like to insert in the record, Mr. Chairman.

[The statement referred to above was not received at press time.]

Mr. **MCMILLEN**. I have some questions that I'd like to follow up on which revolve around DoD's compliance to this Act. In many ways, this Act was designed for DoD; yet, it's not completely logical why they've been so slow to comply.

Again, I want to echo what Congressman Glickman said.

How in your view do they interpret this differently?

Mr. **PLAGER**. I guess I'm not sure that they interpret it differently. I think they have an enormous problem to deal with. And I think, as so often is the case with big agencies with big problems, it's sometimes hard to get their attention at a high enough level and often enough to really move them quickly to address this problem.

We've had meetings with DoD. We recognize their problem. At the same time, we have no intention of giving any slack or allowing them not to fully comply. We have agreed that they need additional time to get through the procedural steps of developing all the plans for all the systems they have.

They've identified I think now and have plans now for some 90—I think it's 93 systems as of the last head count. My guess is there are many more that we need to get plans from them on. They did a preliminary assessment first because of the size of their problem. And they are now following through with the more detailed plans.

And, frankly, Mr. McMillen, I anticipate that there's going to be not an easy job for them or for the rest of us to get all those plans in and get them all up to the quality that they need to be.

But I can assure you we intend to have that happen.

Mr. **MCMILLEN**. Do you feel that maybe DoD felt their security guidelines were sufficient?

Mr. **PLAGER**. I'm sure they felt their security guidelines were sufficient. Everybody within the agency would naturally begin from that position. But I think they understand that they are coming into line with the rest of the government now.

Mr. **MCMILLEN**. They've made great progress. Are they still behind other agencies in terms of submissions?

Mr. PLAGER. I'm not sure how to measure behind. They're the ones with the biggest problem compared to an agency with only a few sensitive systems that was able to get together a few plans and say, Hey, we're pretty well done. DoD is very far from done. In that sense, they're behind.

But, since there is no other agency quite their size and with quite their problems, I can't compare them with anybody else in that position.

Mr. MCMILLEN. And quite their importance.

Mr. PLAGER. And quite their importance.

Mr. MCMILLEN. An auxiliary question. Do you find that with the recent publicity about viruses, hacking and so forth, that we're seeing a greater incidence of this kind of activity?

Mr. PLAGER. There is that concern. I know we have that concern, for example, with FDA activities sometimes. There's always a problem. Do you tell everybody that somebody's out there poisoning aspirin bottles? Does that stimulate other people to do it?

It's sort of the same problem here. Do we go public and say, My goodness, look what some clown's done this week—does that encourage somebody else to do it?

There's always that tension. I think, in this case, there may have been an attitude in the public at one time:

Gee, look at these clever kids who figure out how to break into government computers.

And what was that movie that sort of dramatized the fun of creating War Games, I think was the movie. I'm sure it was done with some basic innocence and entertainment in mind.

But I think that there is a public awareness today of the seriousness of this that may not have existed before. And I think that certainly is true in government.

Mr. MCMILLEN. I introduced legislation earlier this year, the Computer Protection Act, which was trying to stop, put penalties in place, significant criminal fines and penalties, including prison sentences on violators, not only those who send viruses into computers, but they deal from both the software and the hardware side of this problem.

The reason I asked the question about the fact that publicity might be creating greater incidents, the best analogy I can give is the freeway shooters in L.A. It became sort of a rage where people were going down on the highway in California and firing guns out of their windows. The copycat tendency here that is concerning to me. And I hope legislation can be put in place to make sure that there is some teeth to this enforcement.

Thank you.

Mr. VALENTINE. Mr. Rohrabacher.

Mr. ROHRABACHER. I've been in and out, so I think I'll pass.

Mr. VALENTINE. Mr. Campbell.

Mr. CAMPBELL. Just to welcome the Dean and I look forward to working with him. Otherwise, I pass, Mr. Chairman.

Mr. PLAGER. I spent some time at Stanford.

[Laughter.]

Mr. CAMPBELL. Let the record state that you were Dean at a different institution.

Mr. VALENTINE. Thank you very much. I have no intention of starting all of that.

[Laughter.]

Mr. PLAGER. I enjoyed it.

Mr. VALENTINE. We appreciate this very much. Thank you.

The next witness on the list is Admiral Studeman, who has been detained temporarily, so we'll pass over him. I will invite Mr. Raymond G. Kammer to come up, please.

Mr. Kammer is Acting Director of the National Institute of Standards and Technology. We will receive your statement for the record and invite you to proceed by summarizing or any other appropriate way.

Let me say also that Mr. Kammer is accompanied here today by Mr. James Burrows, Director of the National Computer Systems Laboratory.

Welcome.

STATEMENT OF MR. RAYMOND G. KAMMER, ACTING DIRECTOR, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY; ACCOMPANIED BY MR. JAMES BURROWS, DIRECTOR, NATIONAL COMPUTER SYSTEMS LABORATORY

Mr. KAMMER. Thank you. I'll take advantage of your opportunity to summarize my statement and the topics that I'll speak to are the Memorandum of Understanding, the activity of our Computer Systems Security and Privacy Advisory Board, our review of the plans from the agencies for computer security, and the development of guidance on computer security awareness training.

I'll state as sort of a general summary that I hope we've made significant progress. As has already been observed here, the progress is attributable largely to the cooperative attitude and effort of OMB and NSA and NIST.

There are of course some difficult problems still ahead of us, quite a few of them. With respect to the Memorandum of Understanding, as a result of a long and arduous discussion between NIST and NSA, we are now in a position where we'll very shortly sign a Memorandum of Understanding.

In fact, yesterday evening, the Secretary of Commerce gave his approval to my signing the Memorandum of Understanding. And I believe NSA is in a similar position, or will be shortly. So we're very close to it.

Next, I'll bring you up-to-date a little bit on the Computer Systems Security and Privacy Advisory Board. The Board is now organized. They met on March 1st and 2nd. They will have another meeting in May.

In that meeting, the Board will begin review of a strategic plan on NIST activities for implementing the Computer Security Act.

Mr. Burrows, who chaired the first meeting of the Board, will step down as chair and a new chairperson from the private sector will be in place by the May meeting.

With respect to our agency computer security plans, there are five review teams composed of NIST and NSA staff members who are currently reviewing the plans. As of about a week ago, we had 1,543 security plans; 74 of those are from the Department of Defense, and we do expect quite a few more plans from the Department of Defense.

The review process has three phases into which we've currently divided it. The first one is basically logging them in and then we do a preliminary screen to decide what kind of analysis is needed. And then we go into a detailed analysis and preparation of comments.

We've completed the preliminary screening on all 1,500 plus plans and we're in the process of detailed analysis. Only two plans have gone all the way through the process at this point. The lessons that we were learning from the reviewing process are that there's quite a bit left to do. There are quite a few inconsistencies perhaps within agencies as to the nature of their computer security policies.

This is not going to be a simple process. There is a formidable task ahead of us. The review is a worthwhile process, although NSA and NIST staff are finding it somewhat difficult.

We expect our review teams to have completed the review of the plans that we've received so far by this June. Then we expect a second wave of plans from the Department of Defense in August, and we hope to complete the review of those plans in the fall.

In June, we finished the review of the first 1,500 or so plans. We'll prepare summary analyses of the reports; we'll make this available of course to the Committee and to others.

We are going to take a mid-course kind of a look at the planning process next week with the other federal agencies; then we plan a second workshop on July 5th.

The intent of that workshop is to produce sort of a lessons learned document, which will guide us on the future planning, and the future of this process.

We have tasked the agencies. Just the direction we take in doing that is what we hope to learn from this group of plans. We're also preparing a series of technical and management guidelines to try and provide direct technical assistance to the federal agencies. Among the documents that we are currently considering are guidelines to assist executives in planning for computer security, a guide to help them address computer security issues throughout the life cycle of the systems that they purchase and operate, a guide to understanding and using trusted computer system concepts, especially for protecting unclassified federal information, and a series of guides to assist system administrators and the managers in the management, administration and maintenance of the security-related components of their system.

A number of these guides will address problems that have been identified by the President's Council on Integrity and Efficiency. And the most recent study of controls and security needed throughout the process of the system life cycle.

Another implementation activity has been guidance for security awareness training. This has been done with the fullest cooperation and support of the Office of Personnel Management. The first document on the Computer Security Training Guidelines has been issued in draft and will be printed soon. The intent of these guides is to help the agencies determine the training needs.

Also nearing completion is the Computer User's Guide to Protection of Information Assets, which gives managers a way of assessing risks in their system.

The last topic I'd like to address is our support activity to respond to software attacks. We've been working closely with the Department of Defense, with the Department of Justice and NSA on efforts to establish an emergency response capability.

To this end, I've redirected $200,000 this year to help start it up in an effort to coordinate responses, to computer security incidents and create an information clearing house.

In summary, I think we've made a good start. There's a lot more to do. And this is by way of a work in progress report rather than a report that everything is completed or everything is in perfect shape.

[The prepared statement of Mr. Kammer, plus the signed Memorandum of Understanding follow:]

U.S. DEPARTMENT OF COMMERCE
STATEMENT OF RAY KAMMER, DEPUTY DIRECTOR
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
BEFORE THE SUBCOMMITTEE ON
TRANSPORTATION, AVIATION, AND MATERIALS
and
SCIENCE, RESEARCH AND TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES
March 21, 1989

Mr. Chairman and Members of the Subcommittee:

I am here to testify on the National Institute of Standards and Technology's activities to implement the Computer Security Act of 1987. I am accompanied by James H. Burrows, Director of NIST's National Computer Systems Laboratory.

My statement today will cover the following topics: the completion of the Memorandum of Understanding with the National Security Agency; the activities of the Computer System Security and Privacy Advisory Board; the review of agency computer security plans; and the development of guidance on computer security awareness training. I request your permission to insert into the record a discussion of our technical program highlighting some key standards and guidelines.

I believe that NIST has made significant progress in implementing the Computer Security Act. We have met many of the goals that we established for this first year of implementation, and we are continuing to work toward achieving our remaining objectives. Our accomplishments to date stem, in a large part, from the genuine spirit of cooperation that has been displayed by the other agencies that are part of the implementation activities, particularly the Office of Management and Budget (OMB), the Office of Personnel Management (OPM), and the National Security Agency (NSA).

I believe that the Computer Security Act has been effective in stimulating awareness of the need for better computer security in the Federal government. However, there are still tough problems to solve in the years ahead. We want to continue to move forward, and to be the government's leader in finding solutions to the problems related to the protection of unclassified information. I hope that, in the 1990s, we can say that the Federal government leads the nation in developing and using cost effective security controls.

Before covering the specific topics, I would like to give you a picture of our resources for computer security. During the current fiscal year, NIST's computer security program is funded at $2.5 million. This includes $1.5 million for new activities to start implementation of the legislation and $1 million on our ongoing technical program to develop standards, guidelines and technical methods to protect unclassified, sensitive information. As you will recall, from January 1988 when the law was enacted until the beginning of the current fiscal year, we had no additional funding for implementation activities. Our budget request for FY1990 includes an increase of $3.5 million. This amount includes $1.5 million to respond more completely to the requirements of the legislation, and $2 million to augment our technical program to meet future technology challenges. This level of funding will enable us to conduct a focused laboratory-based program, to assist in the development of needed voluntary industry standards, and to provide needed guidance to Federal and private sector computer users. The statement for the record contains details on our program.

I am pleased to report that as a result of much dedicated work on the part of both agencies, NIST and NSA have completed a Memorandum of Understanding (MOU) that will enable us to move forward even further in implementing the Computer Security Act. The MOU grants NSA access to the planning process used by NIST in initiating new research and development projects "to be developed" pertinent to the protection of Federal computer systems in the area of cryptography. These planning exercises typically occur three to five years before drafting begins on a particular standard or guideline. The MOU permits NSA to appeal to the Secretary of Commerce and the Secretary of Defense to review a particular research and development project if NSA deems a particular matter not to be "consistent with the national security of the United States", and recognizes "that such an issue may be referred to the President through the National Security Council for resolution".

The draft MOU provides a number of benefits to NIST and NSA. It allows full implementation of the Computer Security Act of 1987. Both organizations are now free to start work on addressing the significant security issues inherent in the explosion of commputer and communications technologies within the Federal Government. This agreement will allow NIST personnel to develop specific program plans based upon a firm understanding of the respective roles of each ogranization.

Next, I will bring you up to date on the activities of the Computer System Security and Privacy Advisory Board. The Board met on March 1 and 2 to start addressing emerging issues in computer security. The first meeting was devoted primarily to presentations from the Federal sector on current problems in computer security. Members are enthusiastic about their task, and have started in-depth discussions among themselves to address the questions that were posed by this Committee. Although the Board would have liked to have testified today, it felt that it did not have any new insights to share at this time and preferred to look at the problems in more detail in order to develop substantive future reports. The Board requested, and we will deliver for its upcoming May meeting, a strategic plan on NIST activities for implementing the Computer Security Act. Mr. Burrows, who chaired the Board's first meeting, plans to step down as chair. A new chairperson from a private sector organization will be appointed to replace him.

The next topic is our review of agency computer security plans. Five review teams, composed of NIST and NSA staff members, are currently reviewing the computer security plans that were submitted by the Federal agencies. This analysis was preceded by cooperative efforts on the part of OMB, NIST and NSA to develop guidance for the format and content of the plans, and to develop procedures and criteria to guide the reviewers. A copy of the procedures and criteria has already been submitted to the Committee.

As of March 13, we have received 1,543 security plans, 74 from the Department of Defense and the remainder from the civilian agencies. The review process consists of three phases: logging in of the plans as they are received; preliminary screening to facilitate analysis, and detailed analysis and preparation of comments. Currently we have completed the preliminary screening of all of the received plans, and all are receiving detailed analysis. Comments and advice have been returned to two agencies.

The focus of the reviews is to provide factual, constructive, and useful comments, not to grade or judge the plans as good or bad. Some observations that we can make, based on the work that has been done, are:

- We are able to discern some significant information about an agency's overall program from examining plans for individual systems, for example, how well the plans reflect overall agency policies or guidance, or the lack thereof.

- We have found that the information gained from the review of plans constitutes only a portion of the information needed to determine the "security of agency systems." At best we will have a view of the security planning process within the agency. However, it is not possible to know if the plans have been implemented or if security controls are in place.

- Computer security training needs further improvement in most agencies. The computer security plans indicate that training has been limited in depth and scope, and limited to too few staff members in the past.

- There are wide disparities being identified within agencies in terms of the quality and apparent completeness of the computer security planning;

We conclude that, despite the limitations of the review process, the review of plans has been useful and instructive. Much valuable information is being collected, and we are using that information to shape our future programs so that we can address real requirements and situations.

We expect that the review teams will have completed their work of the plans submitted do date in June. Summary analyses and reports on the reviews will be developed, and we will, of course, make their analyses available to this committee. We will be taking a mid-course look at planning process on March 27 when we will hold a workshop for Federal agencies to discuss their experiences with the process and the OMB data call. A second workshop will be held on July 5 to discuss the lessons learned from review process, and to wrap up our current review activities.

With the completion of the review of the first round of plans, we will turn our attention to developing needed technical and management guides, and to providing direct technical assistance to Federal agencies. Among the documents currently being considered for development are: a guide to assist executives, managers and users in planning for computer security of their automated information systems; a guide to address computer security issues throughout the system life cycle through the use of using existing standards, guidelines, and technology; a guide to understanding and using trusted computer system concepts and technology for protecting Federal unclassified information; and a series of guides to assist system administrators and managers in the management, administration and maintenance of the security related components of their systems. These guides will help to address problems identified by the President's Council on Integrity and Efficiency in their most recent study of controls and security needed throughout the data processing systems life cycle.

Another implementation activity has been the development of guidance on security awareness training. This has been done with the close cooperation and support of the Office of Personal Management. The first document "Computer Security Training Guidelines" has been issued in draft and will be printed soon. This guidelines will assist agencies in selecting which employees require training and what training they should receive. The guidelines specify training content areas for specific target audiences including users, managers, and executives. Agencies will use this information to enhance their training programs to better meet their specific needs. The Office of Personnel Management (OPM) is already using this framework to develop computer security courses.

Also nearing completion is the "Computer User's Guide to the Protection of Information Assets." This booklet is the first of three security awareness guides, targeted for executives, managers, and users. It covers threats that are inherent to automated information systems, ways to determine risks, and good practices for reducing risks.

The last topic that I want to discuss is our support activity to respond to malicious software attacks. We have been working closely with DoD, DoJ, and NSA on efforts to establish an emergency response capability. For the current fiscal year I have redirected $200,000 to start up an effort to coordinate responses to computer security incidents and to create an information clearinghouse.

We also have contributed to the study being conducted by OMB to assess both the short-term and long-term capabilities needed to prevent future attacks and to assure the continuity of government information processing activities.

In summary, Mr. Chairman, I believe that a good start has been made in implementing the Computer Security Act, that this progress results from the cooperative efforts of many Federal organizations, but that much more remains to be done to make the Federal government's information and information processing activities secure. I thank you for your support and invite any questions that the Committee might have.

Attachment

National Institute of Standards and Technology Computer Security Program

Since the early 1970's, NIST has conducted a laboratory-based computer security program to develop of cost-effective solutions for protecting unclassified information. These solutions are made available to Federal and private organizations through the development and publication of standards, guidelines, and other technical documents; sponsorship of conferences and workshops; and other technology transfer activities. A list of NCSL publications is attached to this testimony.

While the focus of the program in the 1970's was on large mainframe systems, this soon shifted to encompass minicomputers, microcomputers and, more recently, to networks of heterogenous host systems. In addition to the security planning, training, and awareness activities and the establishment of the response and resource centers, all described above, other management and technical areas addressed by NIST's current program include the following:

Risk Management

Implementation of effective information security measures must be based on a balance between cost of controls and the need to reduce risk or expected loss to acceptable levels. To assist Federal agencies in achieving this balance, NIST is working jointly with NSA to investigate risk management techniques that will help agencies identify risks and select cost effective control measures. Specific activities include: 1) establishment of a risk management research laboratory at NIST to study current risk management tools, to develop "standard scenarios" to be used in comparing alternative tools, and to develop guidance documents on the selection of risk management procedures, 2) research to develop a risk management framework for defining the elements of risk management and the functional relationships between the elements, and 3) an annual workshop on risk management models.

Security Management, Evaluation and Audit

To be most effective, security requirements must be considered throughout the entire life cycle of a system. This approach to security has long been central to NIST programs and guidance, and is reflected in many of NIST's publications, including FIPS 73, Guidelines for Security of Computer Applications, FIPS 102, Guideline for Computer Security Certification and Accreditation, and a recently published Special Publication 500-153, Guide for Auditing for Controls and Security: A System Development Life-Cycle Approach. We plan issuance of continued guidance in this area including a series of publications on effective management of various types of specific computer security technologies (for example, operating system access controls).

Security Capabilities in Operating Systems and Databases

Computer technology can itself be part of the solution to the problem of protecting computers and the data they handle. To the maximum extent practical, automated security features and mechanisms should be built into computer operating systems, applications, and databases. Such mechanisms, when combined with more traditional administrative and physical security measures can provide comprehensive and cost-effective data protection. The development and application of such internal, system security features have long been a key element in NIST's computer security program.

System and Integrity

Computer security requires much more than keeping confidential data out of the wrong hands. Indeed, perhaps the most important need is for methods and mechanism to ensure that data (and the programs that handle such data) are protected from unauthorized modification or corruption. Recent research efforts are helping to develop a better understanding of data and system integrity requirements and to develop formal models through which integrity enforcement mechanisms can be built into systems. NIST is leading a joint government and industry effort, the Data Integrity Workshop to develop such methods and mechanisms. This promises to have important and far-reaching benefits in both government and private sectors.

Security Interfaces for POSIX

NIST, in conjunction with the IEEE P1003 (POSIX) standards committee, is working to provide a hardware-independent functional interface specifications for portable application programs. POSIX, when fully developed, will be a family of

Attachment

standards that will support source code portability for a wide range of applications across many different machines and operating systems. Interfaces to standard security functions are key to this effort. NIST has been chairing the P1003.6 security working group which is developing such standards. The result of this effort will be standard security mechanisms available to application programs across a wide range of systems.

Evaluation Criteria

The DoD Trusted System Evaluation Criteria (the "Orange Book"), issued by NSA, describe basic computer security features for computer operating systems and provide criteria for evaluating levels of trust in such systems. In many cases, these criteria can be used to specify system security or trust requirements for non-DoD systems. NIST works with NSA and with agencies to help determine the applicability of these or other criteria to sensitive applications and to develop enhancements that will enable such criteria to be useful to a broader community of users and environments.

Network Security Architectures and Standards for Open Systems

The Open System Interconnection (OSI) standards, that are being adopted by both government and industry, make it possible to interconnect computer systems manufactured by different vendors for data communications through networks. For the past few years, NIST has been addressing the challenge to define the security components that assure confidentiality, integrity, and availability of transmitted data and to identify ways to make systems that are secure as well as "open".

NIST is working with industry and users through the NIST Workshop for Implementors of OSI to identify the needed security standards. In addition, NIST is working with the NSA to assure that security standards developed for open systems also will meet Department of Defense requirements for protecting classified and intelligence data. With support from NSA, NIST has developed a laboratory to test and demonstrate network security protocols.

Attachment

National Institute of Standards and Technology
Computer Security Program

Data Encryption

Recognizing that the increased use of computer networks would lead to a corresponding increase in the need for cryptographic security and that future business transactions between buyer, seller, and banker will be performed electronically with automated communications, NIST issued FIPS 46, Data Encryption Standard (DES), in 1977. FIPS 46 specifies an encryption algorithm for protecting unclassified data. Since that time, NIST has worked within in the ANSI voluntary standards arena to developed additional DES related standards including ANSI X9.9, Message Authentication, ANSI X9.17, Key Management, ANSI X3.106, DES Modes of Operation, ANSI X9.23, Financial Institution Encryption; and ANSI X12.42, Electronic Data Interchange Security Structures.

Although DES was originally intended for Government applications, it has become widely used by industry as well. Many organizations, including the banking community and several Federal agencies, have made large investments in DES technology. To support the use of DES by both the Federal and private sectors, NIST continues to validate commercial devices for correct implementation of the DES algorithm.

Key Management

Since the DES is a publicly known algorithm, the security of the data protected by DES depends upon the protection afforded to the generation and distribution of the secret keys. NIST's work with ANSI to develop standards for managing the secret keys has resulted in the American National Standard for Financial Key Management (ANSI X9.17-1985). In addition, NIST has assisted the Department of Treasury in implementing a validation system that test commercial devices for conformance to the key management standard.

Message Authentication

The DES is also the basis for the American National Standard for Wholesale Financial Institution Message Authentication, ANSI X9.9-1986 and Retail Financial Institution Message Authentication, ANSI X9.19-1985. The standard has also been issued as FIPS 113, Computer Data Authentication. These standards make it possible to detect unauthorized alteration to computer data. Products which implement these standards are used to protect EFT messages worth trillions of dollars.

In 1984, the Department of Treasury issued a policy requiring that the Department's Electronic Funds Transfer Messages be authenticated using ANSI X9.9. To assist Treasury in certifying vendor devices for proper operation, NIST developed a Message Authentication Code (MAC) Validation system. The validation process provides a rigorous, economical, automated test that can be performed at a remote location via dial-up facilities.

Electronic Certification

Another cryptographic procedure based upon the DES provides a way to identify the originator of an electronic form or document and to verify that the contents of the form has not been changed. Known as electronic certification, this procedure replaces the written signature that is used in paper-based systems to make a verifiable link between a document and a person responsible for that document. NIST has worked with the Department of Treasury to develop an Electronic Certification Prototype System (ECPS) which employs a digital message authentication code in place of a written signature. The cryptographic portions of the ECPS rely on standards developed by NIST and products validated by NIST. In September of 1987, the first payment of U.S. Government funds not requiring a written signature was disbursed from a system currently being used between the Executive Office of the President and Treasury. NIST would like to assist other agencies in developing applications that use electronic certification technology.

Network Access Control

While most computer systems use passwords to authenticate the identity of users, experience has demonstrated that passwords are often used incorrectly, providing little or no protection from unauthorized access to computer systems and networks. FIPS 112, Password Usage Standard, helps users improve the level of protection provided by passwords.

NIST has been investigating the use of integrated circuit (IC) technology (e.g., smart tokens, smart cards, hand held plastic devices) for controlling access to systems. The tokens and cards can be used to store and transport the secret cryptographic keys needed in electronic certification systems.

Recent NIST research activities have focused on the use of smart cards for controlling access to computer networks. Initial findings are published in Special Publication 500-157, Smart Card Technology: New Methods for Computer Access Control. This document contains a description of a NIST developed prototype system which uses a password, a smart card, a biometrics fingerprint reader, and cryptography to control access to a computer system. In addition, a project to research and develop prototype smart card access control systems has been started under the sponsorship of the Defense Advanced Research Projects Agency (DARPA). These systems will eliminate several of the weaknesses found in password-based systems used today and will significantly reduce the likelihood of successful hacker penetrations.

Future Plans

As computer system architectures move from networked heterogenous systems to full distributed processing environments where the distinction between computers and telecommunications disappear and data, voice, fax, and video are all digitally encoded (e.g., ISDN), all aspects of protecting information resources become more complex. These include:

- definition and enforcement of consistent security policies
- user identification and authentication
- authorization and access control to information resources
- secure communications protocols and services
- system reliability and recoverability
- audit trail collection and threat monitoring, including analysis and variance detection
- secure distributed data base architectures
- risk analysis/management of distributed systems

Attachment

National Institute of Standards and Technology Computer Security Program

NIST's broad-based experience in computer and telecommunications security place it in an excellent position to launch an extensive and highly integrated approach to developing the management and technical methods necessary to transition government and industry from today's networked systems to future distributed processing environments. To meet this challenge, the FY 1990 budget submission to Congress proposes a NIST research program that provides a balance of several key activities including:

- laboratory-based research
- development of cost-effective management and technical security methods and solutions
- leadership in developing national and international information security standards
- encouragement and facilitation of technology transfer
- development of materials to support security awareness and training.

The experience gained by NIST in addressing current system architectures provides the solid technical foundation necessary for developing new technologies and cost-effective techniques for assuring secure distributed computing. Key technical areas that NIST plans to address include:

Risk Analysis/Management

Research and development must be conducted leading to improved methods for evaluating and managing risk in distributed systems. These include automated risk management tools; contingency planning; security policy models; security planning, training, and awareness; and audit trail collection, analysis, and variance detection.

Security Services and Standards for OSI, ISDN, and Other Open System Architectures

NIST's current laboratory-based activities will be expanded to support the development and prototype implementations of techniques leading to standards in open systems such as OSI and ISDN. This joint activity between Government and private sector users and vendors will result in national/international standards and conformance test procedures. The goal of this activity is to assure that vendors incorporate emerging standards into their open system products so that Federal and private sector users obtain security protection and interoperability from the procured network products.

To leverage congressionally mandated activities, NIST is establishing an innovative program for bringing together government organizations and private contractors interested in interoperability and security in the OSI computer network architecture and the ISDN communications architecture. This program, announced in the January 30, 1989 issue of the Commerce Business Daily, has as its objectives:

- to develop demonstration prototypes of applications and equipment, including hardware and software, that provide one or more levels of security in an OSI and/or ISDN environment, and
- to develop data formats, protocols, interfaces, and support systems for security in an OSI/ISDN environment that can be used as a basis for Federal Information Processing Standards. Such standards may then be used as bases for Federal procurement of services and systems in the future, and;
- to provide a laboratory in which users, developers, and vendors can jointly define, develop, and test systems that will provide a range of telecommunications, network management, and security services in a distributed information processing environment.

Identification, Authentication, and Access Controls

Current identification, authentication, and access control techniques need to be expanded and applied to distributed systems. These include token-based authentication (e.g., smart cards), digital signatures, message authentication, public key cryptography, and key management.

Attachment

National Institute of Standards and Technology
Computer Security Program

Systems Engineering for Reliability and Security

Since the complexity and scope of distributed processing systems places them at a far greater risk or compromise of system and data integrity, better techniques need to be used in developing safe, secure, and reliable systems. Such techniques include specification methodologies, methods for automating software production based on design specifications, and verification and test methods to ascertain the correctness/quality of developmental and operational systems.

Security Functionality in Operating Systems

Research and development will focus on operating system functionality, operating systems architectures to support distributed environments, interfaces between trusted operating systems and other components of open system environments, and cost/benefit trade-offs in using trusted operating systems in such environments.

Distributed Database Architectures

Since one of the key requirements for distributed computing systems is to support widely distributed information processing functions of an organization, new database architectures and management systems need to be developed to support these environments. Research and development will focus on database architectures, management systems, and techniques to ensure that the confidentiality, integrity, and availability of geographically distributed databases are maintained and that users of databases are prevented from statistically inferring new information (that they are not authorized to know) from bits and pieces of information they are authorized to know.

COMPUTER SECURITY PUBLICATIONS

PUBLICATIONS LIST 91

FEBRUARY 1989

U.S DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
NATIONAL COMPUTER SYSTEMS LABORATORY

NATIONAL COMPUTER SYSTEMS LABORATORY

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
GAITHERSBURG, MARYLAND 20899

The National Computer Systems Laboratory (NCSL) is responsible for developing standards, providing technical assistance, and conducting research for computers and related systems. These activities provide technical support to government and industry in the effective, safe and economical use of computers. NCSL's work is mandated under the Brooks Act (P.L. 89-306) and the Computer Security Act of 1987 (P.L. 100-235). NCSL's activities also support key goals of the Department of Commerce: to maintain a U.S. competitive position in international trade; to improve U.S. productivity; and to improve the management of government and the delivery of services.

NCSL's major activities are:

- o determining requirements for and participating in the development of national and international voluntary industry standards for computers and related telecommunications;
- o developing testing methodologies to support the development and implementation of standards;
- o developing guidelines, technology forecasts, and other products to aid in the effective management and application of computer and related telecommunications technology;
- o disseminating and exchanging information with Federal, State and local governments, industry, professional, and research organizations on computer use and standards needs;
- o providing technical support for the development of government policies in information technology;
- o providing direct technical assistance to Federal agencies on a cost reimbursable basis;
- o carrying out applied research and development, often in cooperation with other government agencies and with industry.

COMPUTER SECURITY ACTIVITIES

NCSL's responsibilities were reaffirmed and strengthened by the enactment of the Computer Security Act of 1987 (P.L. 100-235). This legislation tasks NCSL to perform research, develop standards and guidelines, develop validation procedures for standards, assist the Federal agencies and the private sector, and assist Federal agencies with their security planning and training activities.

Computer security is important to managers and users of information systems. Security is the tool for achieving integrity and accuracy of data, confidentiality of information handled by systems, and the availability of systems, data, and services. Many different accidental and intentional events can threaten security. NCSL identifies and develops cost-effective methods to protect computers and data against all types of losses. These methods include technical solutions to computer security problems, as well as sound management practices.

HOW TO ORDER PUBLICATIONS

These publications are available through the Government Printing Office (GPO) and the National Technical Information Service (NTIS). The source and price for each publication are indicated. Orders for publications should include title of publication, NIST publication number (Spec. Pub. 000, Tech. Note 000, etc.) and NTIS or GPO number. Your may order at the price listed; however, prices are subject to change without notice.

Submit payment in the form of postal money order, express money order or check made out to the Superintendent of Documents for GPO-stocked documents or to the National Technical Information Service for NTIS-stocked documents.

Mailing addresses are:

Superintendent of Documents
U.S. Government Printing Office
Washington, DC 20402

National Technical Information Service
5285 Port Royal Road
Springfield, VA 22161

Telephone numbers for information are:

GPO Order Desk	(202) 783-3238
NTIS Orders	(703) 487-4780
NTIS Information	(703) 487-4600

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATIONS (FIPS)

Federal Information Processing Standards Publications (FIPS PUBS) are developed by the National Computer Systems Laboratory (NCSL) and issued under the provisions of the Federal Property and Administrative Services Act of 1949, as amended; and Public Law 89-306 (79 Stat. 1127), as amended.

FIPS PUBS are sold by the National Technical Information Service (NTIS), U.S. Department of Commerce. A list of current FIPS covering all NCSL program areas is available from:

Standards Processing Coordinator (ADP)
National Computer Systems Laboratory
Technology Building, B-64
National Institute of Standards and Technology
Gaithersburg, MD 20899
Phone: (301) 975-2817

FIPS PUB 31

GUIDELINES FOR ADP PHYSICAL SECURITY AND RISK MANAGEMENT
June 1974

Provides guidance to Federal organizations in developing physical security and risk management programs for their ADP facilities. Covers security analysis, natural disasters, failure of supporting utilities, system reliability, procedural measures and controls, protection of off-site facilities, contingency plans security awareness, and security audit. Can be used as a checklist for planning and evaluating security of computer systems.

FIPS PUB 39

GLOSSARY FOR COMPUTER SYSTEMS SECURITY
February 1974

A reference document containing approximately 170 terms and definitions pertaining to privacy and computer security.

FIPS PUB 41

COMPUTER SECURITY GUIDELINES FOR IMPLEMENTING THE PRIVACY ACT OF 1974
May 1975

Provides guidance in the selection of technical and related procedural methods for protecting personal data in automated information systems. Discusses categories of risks and the related safeguards for physical security, information management practices, and system controls to improve system security.

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATIONS (cont.)

FIPS PUB 46-1	DATA ENCRYPTION STANDARD January 1988 (Reaffirmed until 1992) Specifies an algorithm to be implemented in electronic hardware devices and used for the cryptographic protection of sensitive, but unclassified, computer data. The algorithm uniquely defines the mathematical steps required to transform computer data into a cryptographic cipher and the steps required to transform the cipher back to its original form. This standard has been adopted as a voluntary industry standard ANSI X3.92-1981/R1987
FIPS PUB 48	GUIDELINES ON EVALUATION OF TECHNIQUES FOR AUTOMATED PERSONAL IDENTIFICATION April 1977 Discusses the performance of personal identification devices, how to evaluate them and considerations for their use within the context of computer system security.
FIPS PUB 65	GUIDELINE FOR AUTOMATIC DATA PROCESSING RISK ANALYSIS August 1979 Presents a technique for conducting a risk analysis of an ADP facility and related assets. Provides guidance on collecting, quantifying, and analyzing data related to the frequency of caused by adverse events. This guideline describes the characteristics and attributes of a computer system that must be known for a risk analysis and gives an example of the risk analysis process.
FIPS PUB 73	GUIDELINES FOR SECURITY OF COMPUTER APPLICATIONS June 1980 Describes the different security objectives for a computer application, explains the control measures that can be used, and identifies the decisions that should be made at each stage in the life cycle of a sensitive computer application. For use in planning, developing and operating computer systems which require protection. Fundamental security controls such a data validation, user identity verification, authorization, journalling, variance detection, and encryption are discussed.

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATIONS (cont.)

FIPS PUB 74	GUIDELINES FOR IMPLEMENTING AND USING THE NBS DATA ENCRYPTION STANDARD April 1981 Provides guidance for the use of cryptographic techniques when such techniques are required to protect sensitive or valuable computer data. For use in conjunction with FIPS PUB 46 and FIPS PUB 81.
FIPS PUB 81	DES MODES OF OPERATION December 1980 Defines four modes of operation for the Data Encryption Standard which may be used in a wide variety of applications. The modes specify how data will be encrypted (cryptographically occurrence and the damage protected) and decrypted (returned to original form). The modes included in this standard are the Electronic Codebook (ECB) mode, the Cipher Block Chaining (CBC) mode, the Cipher Feedback (CFB) mode, and the Output Feedback (OFB) mode.
FIPS PUB 83	GUIDELINE ON USER AUTHENTICATION TECHNIQUES FOR COMPUTER NETWORK ACCESS CONTROL September 1980 Provides guidance in the selection and implementation of techniques for authenticating the users of remote terminals in order to safeguard against unauthorized access to computers and computer networks. Describes use of passwords, identification tokens, verification by means of personal attributes, identification of remote devices, role of encryption in network access control, and computerized authorization techniques.
FIPS PUB 87	GUIDELINES FOR ADP CONTINGENCY PLANNING March 1981 Describes what should be considered when developing a contingency plan for an ADP facility. Provides a suggested structure and format which may be used as a starting point from which to design a plan to fit each specific operation.

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATIONS (cont.)

FIPS PUB 88	GUIDELINE ON INTEGRITY ASSURANCE AND CONTROL IN DATABASE APPLICATIONS August 1981 Provides explicit advice on achieving database integrity and security control. Identifies integrity and security problems and discusses procedures and methods which have proven effective in addressing these problems. Provides an explicit, step-by-step procedure for examining and verifying the accuracy and completeness of a database.
FIPS PUB 94	GUIDELINE ON ELECTRICAL POWER FOR ADP INSTALLATIONS September 1982 Provides information on factors in the electrical environment that affect the operation of ADP systems. Describes the fundamentals of power, grounding, life-safety, static electricity, and lightning protection requirements, and provides a checklist for evaluating ADP sites.
FIPS PUB 102	GUIDELINE FOR COMPUTER SECURITY CERTIFICATION AND ACCREDITATION September 1983 Describes how to establish and how to carry out a certification and accreditation program for computer security. Certification consists of a technical evaluation of a sensitive system to see how well it meets its security requirements. Accreditation is the official management authorization for the operation of the system and is based on the certification process.
FIPS PUB 112	STANDARD ON PASSWORD USAGE May 1985 This standard defines ten factors to be considered in the design, implementation and use of access control systems that are based on passwords. It specifies minimum security criteria for such systems and provides guidance for selecting additional security criteria for password systems which must meet higher security requirements.

FIPS PUB 113 STANDARD ON COMPUTER DATA AUTHENTICATION
May 1985

This standard specifies a Data Authentication Algorithm (DAA) which, when applied to computer data, automatically and accurately detects unauthorized modifications, both intentional and accidental. Based on the Data Encryption Standard (DES), this standard is compatible with requirements adopted by the Department of Treasury and the banking community to protect electronic fund transfer transactions.

SPECIAL PUBLICATIONS AND OTHER REPORTS

These publications present the results of NCSL studies, investigations, and research on computer security and risk management issues. Publications are sold by either the Government Printing Office or the National Technical Information Service. Prices and stock numbers are listed at the back of this brochure.

SPECIAL PUBLICATIONS

NBS SPEC PUB
500-158

ACCURACY, INTEGRITY, AND SECURITY IN COMPUTERIZED VOTE-TALLYING
By Roy G. Saltman
August 1988

This study surveys some events concerning computerized vote-tallying and reviews current problems. The report recommends that accepted practices of internal control be applied to vote-tallying, including: use of software for integrity and logical correctness; dedicated software use and dedicated operation; improved design and certification of vote-tallying systems that do not use ballots; and improved pre-election testing and partial manual recounting of ballots.

NBS SPEC PUB
500-157

SMART CARD TECHNOLOGY: NEW METHODS FOR COMPUTER ACCESS CONTROL
By Martha E. Haykin and Robert B. J. Warner
September 1988

This document describes the basic components of a smart card and provides background information on the underlying integrated circuit technologies. The capabilities of a smart card are discussed, especially its applicability for computer security. The report describes research being conducted on smart card access control techniques; other major U.S. and international groups involved in the development of standards for smart cards and related devices are outlined in the appendix.

NBS SPEC PUB 500-156

MESSAGE AUTHENTICATION CODE (MAC) VALIDATION SYSTEM: REQUIREMENTS AND PROCEDURES
By Miles Smid, Elaine Barker, David Balenson and Martha Haykin
May 1988

Describes the Message Authentication Code (MAC) Validation System (MVS) which was developed by NBS to test message authentication devices for conformance to two data authentication standards (including FIPS 113). This publication describes the basic design and configuration of the MVS, and the requirements and administrative procedures to be followed for requesting validations.

NBS SPEC PUB 500-153

GUIDE TO AUDITING FOR CONTROLS AND SECURITY: A SYSTEM DEVELOPMENT LIFE CYCLE APPROACH
Editors/Authors: Zella G. Ruthberg, Bonnie T. Fisher, William E. Perry, John W. Lainhart IV, James G. Cox, Mark Gillen, and Douglas B. Hunt
April 1988

This guide describes a process for auditing the system development life cycle (SDLC) of an automated information system (AIS) to ensure that controls and security are designed and built into the system. The guide was developed by the Electronic Data Processing (EDP) Systems Review and Security Work Group of the Computer Security Project within the President's Council on Integrity and Efficiency (PCIE), and contains bibliographies, and a description of pertinent laws and regulations.

NBS SPEC PUB 500-137

SECURITY FOR DIAL-UP LINES
By Eugene F. Troy
May 1986

Ways to protect computers from intruders via dial-up telephone lines are discussed in this guide. Highlighted are hardware devices which can be fitted to computers or used with their dial-up terminals to provide communications protection for non-classified computer systems. Six different types of hardware devices and the ways that they can be used to protect dial-up computer communications are described. Also discussed are techniques that can be added to computer operating systems or incorporated into system management or administrative procedures.

SPECIAL PUBLICATIONS (Cont.)

NBS SPEC PUB
500-134

GUIDE ON SELECTING ADP BACKUP PROCESS ALTERNATIVES
By Irene Isaac
November 1985

Discusses the selection of ADP backup processing support in advance of events that cause the loss of data processing capability. Emphasis is placed on management support at all levels of the organization for planning, funding, and testing of an alternate processing strategy. The alternative processing methods and criteria for selecting the most suitable method are presented, and a checklist for evaluating the suitability of alternatives is provided.

NBS SPEC PUB
500-133

TECHNOLOGY ASSESSMENT; METHODS FOR MEASURING THE LEVEL OF COMPUTER SECURITY
By William Neugent, John Gilligan, Lance Hoffman, and Zella G. Ruthberg
October 1985

The document covers methods for measuring the level of computer security, i.e. technical tools or processes which can be used to help establish positive indications of security adequacy in computer applications, systems, and installations. The report addresses individual techniques and approaches, as well as broader methodologies which permit the formulation of a composite measure of security that uses the results of these individual techniques and approaches.

NBS SPEC PUB
500-121

GUIDANCE ON PLANNING AND IMPLEMENTING COMPUTER SYSTEMS RELIABILITY
By Lynne S. Rosenthal
January 1985

This report presents guidance to managers and planners on the basic concepts of computer system reliability and on the implementation of a management program to improve system reliability. Topics covered include techniques for quantifying and evaluating data to measure system reliability, designing systems for reliability, and recovery of a computer system after it has failed or produced erroneous output. An appendix contains references and a list of selected readings.

SPECIAL PUBLICATIONS (Cont.)

NBS SPEC PUB 500-120

SECURITY OF PERSONAL COMPUTER SYSTEMS - A MANAGEMENT GUIDE
By Dennis D. Steinauer
January 1985

This publication provides practical advice on the following issues: physical and environmental protection system and data access control; integrity of software and data; backup and contingency planning; auditability; communications protection. References to additional information, a self-audit checklist, and a guide to security products for personal computers are included in the appendices.

NBS SPEC PUB 500-109

OVERVIEW OF COMPUTER SECURITY CERTIFICATION AND ACCREDITATION
By Zella G. Ruthberg and William Neugent
April 1984

This publication is a summary of and a guide to FIPS PUB 102, Guideline to Computer Security Certification and Accreditation. It is oriented toward the needs of ADP policy managers, information resource managers, ADP technical managers, and ADP staff in understanding the certification and accreditation process.

NBS SPEC PUB 500-85

EXECUTIVE GUIDE TO ADP CONTINGENCY PLANNING
By James K. Shaw and Stuart W. Katzke
July 1981

This document provides, in the form of questions and answers, the background, and basic essential information required to understand the developmental process for automatic data processing (ADP) contingency plans. The primary intended audience consists of executives and managers who depend on ADP resources and services, yet may not be directly responsible for the daily management or supervision of data processing activities or facilities.

NBS SPEC PUB 500-67

THE SRI HIERARCHICAL DEVELOPMENT METHODOLOGY (HDM) AND ITS APPLICATION TO THE DEVELOPMENT OF SECURE SOFTWARE
By Karl N. Levitt, Peter Neumann, and Lawrence Robinson
October 1980

Describes the SRI Hierarchical Development Methodology for designing large software systems such as operating systems and data management systems that must meet stringent security requirements.

NBS SPEC PUB 500-61

MAINTENANCE TESTING FOR THE DATA ENCRYPTION STANDARD
By Jason Gait
August 1980

Describes four tests that can be used by manufacturers and users to check the operation of data encryption devices. These tests are simple, efficient, and independent of the implementation of the Data Encryption Standard (FIPS 46).

NBS SPEC PUB 500-57

AUDIT AND EVALUATION OF COMPUTER SECURITY II: SYSTEM VULNERABILITIES AND CONTROLS
Edited by Zella G. Ruthberg
April 1980

Proceedings of the second NBS/GAO workshop to develop improved computer security audit procedures. Covers eight sessions: three sessions on managerial and organizational vulnerabilities and controls and five technical sessions on terminals and remote peripherals, communication components, operating systems, applications and non-integrated data files, and data base management systems.

NBS SPEC PUB 500-54

A KEY NOTARIZATION SYSTEM FOR COMPUTER NETWORKS
By Miles E. Smid
October 1979

Describes a system for key notarization, which can be used with an encryption device, to improve data security in computer networks. The key notarization system can be used to communicate securely between two users, communicate via encrypted mail, protect personal files, and provide a digital signature capability.

OTHER REPORTS

NBSIR 86-3386

WORK PRIORITY SCHEME FOR EDP AUDIT AND COMPUTER SECURITY REVIEW
By Zella Ruthberg and Bonnie Fisher
August 1986

This publication describes a methodology for prioritizing the work performed EDP auditors and computer security reviewers. Developed at an invitational workshop attended by government and private sector experts, the work plan enables users to evaluate computer systems for both EDP audit and security review functions and to develop a measurement of the risk of the systems. Based on this measure of risk, the auditor can then determine where to spend review time.

SUBJECT INDEX

Contingency Planning

FIPS PUB 87
SPEC PUB 500-85

Database Security

FIPS PUB 88

Encryption

FIPS PUB 46-1
FIPS PUB 74
FIPS PUB 81
FIPS PUB 113
SPEC PUB 500-54
SPEC PUB 500-61
SPEC PUB 500-156

Evaluation of Computer Security

FIPS PUB 102
SPEC PUB 500-57
SPEC PUB 500-109
SPEC PUB 500-153
NBSIR 86-3386

General Computer Security

FIPS PUB 39
FIPS PUB 73
FIPS PUB 112
SPEC PUB 500-120
SPEC PUB 500-137
SPEC PUB 500-157
SPEC PUB 500-158

Network Security

SPEC PUB 500-54

Physical Security

FIPS PUB 31

Power, Grounding, and Life Safety

FIPS PUB 94

Privacy

FIPS PUB 41
SPEC PUB 500-50

Risk Management

FIPS PUB 31
FIPS PUB 65

Software and Operating Systems

SPEC PUB 500-67
SPEC PUB 500-121
SPEC PUB 500-134

User Authentication

FIPS PUB 48
FIPS PUB 83

RAYMOND G. KAMMER

Acting Director
National Institute of Standards and Technology (NIST)
(Formerly National Bureau of Standards (NBS)
United States Department of Commerce

Ray Kammer is Deputy Director of NIST. He is currently Acting Director as well. NIST is the Nation's central laboratory for measurement and standards research in support of U.S. industrial needs. Kammer manages the NIST staff of close to 3100 physicists, chemists, mathematicians, engineers, and support personnel.

A graduate of the University of Maryland, Kammer joined NIST in 1969 as a technical program analyst. Over the following decade he served the agency and the U.S. Department of Commerce in a succession of offices concerned with budgetary and program analysis; planning; and personnel management. In 1980, Kammer was appointed Deputy Director of NIST.

In addition, Kammer has served as chairman of several important evaluation committees for the Department of Commerce, including reviews of satellite systems for weather monitoring and the U.S. LANDSAT program, and the next generation of weather radars used by the U.S. government. He is now serving a three-year term on the Board of Directors of ASTM, a major international organization for the development of voluntary standards for materials, products, systems and services.

His awards include both the Gold and Silver medals of the Department of Commerce, given for meritorious service to the Department and the nation, the William A. Jump Award for Exceptional Achievement in Public Administration, the Federal Government Meritorious Executive Award, and the Roger W. Jones Award for Executive Leadership.

February 1989

MEMORANDUM OF UNDERSTANDING
BETWEEN
THE DIRECTOR OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
AND
THE DIRECTOR OF THE NATIONAL SECURITY AGENCY
CONCERNING
THE IMPLEMENTATION OF PUBLIC LAW 100-235

Recognizing that:

A. Under Section 2 of the Computer Security Act of 1987 (Public Law 100-235), (the Act), the National Institute of Standards and Technology (NIST) has the responsibility within the Federal Government for:

1. Developing technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems as defined in the Act; and,

2. Drawing on the computer system technical security guidelines of the National Security Agency (NSA) in this regard where appropriate.

B. Under Section 3 of the Act, the NIST is to coordinate closely with other agencies and offices, including the NSA, to assure:

1. Maximum use of all existing and planned programs, materials, studies, and reports relating to computer systems security and privacy, in order to avoid unnecessary and costly duplication of effort; and,

2. To the maximum extent feasible, that standards developed by the NIST under the Act are consistent and compatible with standards and procedures developed for the protection of classified information in Federal computer systems.

C. Under the Act, the Secretary of Commerce has the responsibility, which he has delegated to the Director of NIST, for appointing the members of the Computer System Security and Privacy Advisory Board, at least one of whom shall be from the NSA.

Therefore, in furtherance of the purposes of this MOU, the Director of the NIST and the Director of the NSA hereby agree as follows:

I. The NIST will:

1. Appoint to the Computer Security and Privacy Advisory Board at least one representative nominated by the Director of the NSA.

2. Draw upon computer system technical security guidelines developed by the NSA to the extent that the NIST determines that such guidelines are consistent with the requirements for protecting sensitive information in Federal computer systems.

3. Recognize the NSA-certified rating of evaluated trusted systems under the Trusted Computer Security Evaluation Criteria Program without requiring additional evaluation.

4. Develop telecommunications security standards for protecting sensitive unclassified computer data, drawing upon the expertise and products of the National Security Agency, to the greatest extent possible, in meeting these responsibilities in a timely and cost effective manner.

5. Avoid duplication where possible in entering into mutually agreeable arrangements with the NSA for the NSA support.

6. Request the NSA's assistance on all matters related to cryptographic algorithms and cryptographic techniques including but not limited to research, development, evaluation, or endorsement.

II. The NSA will:

1. Provide the NIST with technical guidelines in trusted technology, telecommunications security, and personal identification that may be used in cost-effective systems for protecting sensitive computer data.

2. Conduct or initiate research and development programs in trusted technology, telecommunications security, cryptographic techniques and personal identification methods.

3. Be responsive to the NIST's requests for assistance in respect to all matters related to cryptographic algorithms and cryptographic techniques including but not limited to research, development, evaluation, or endorsement.

4. Establish the standards and endorse products for application to secure systems covered in 10 USC Section 2315 (the Warner Amendment).

5. Upon request by Federal agencies, their contractors and other government-sponsored entities, conduct assessments of the hostile intelligence threat to federal information systems, and provide technical assistance and recommend endorsed products for application to secure systems against that threat.

III. The NIST and the NSA shall:

1. Jointly review agency plans for the security and privacy of computer systems submitted to NIST and NSA pursuant to section 6(b) of the Act.

2. Exchange technical standards and guidelines as necessary to achieve the purposes of the Act.

3. Work together to achieve the purposes of this memorandum with the greatest efficiency possible, avoiding unnecessary duplication of effort.

4. Maintain an ongoing, open dialogue to ensure that each organization remains abreast of emerging technologies and issues effecting automated information system security in computer-based systems.

5. Establish a Technical Working Group to review and analyze issues of mutual interest pertinent to protection of systems that process sensitive or other unclassified information. The Group shall be composed of six federal employees, three each selected by NIST and NSA and to be augmented as necessary by representatives of other agencies. Issues may be referred to the group by either the NSA Deputy Director for Information Security or the NIST Deputy Director or may be generated and addressed by the group, upon approval by the NSA DDI or NIST Deputy Director. Within 14 days of the referral of an issue to the Group by either the NSA Deputy Director for Information Security or the NIST Deputy Director, the Group will respond with a progress report and plan for further analysis, if any.

6. Exchange work plans on an annual basis on all research and development projects pertinent to protection of systems that process sensitive or other unclassified information, including trusted technology, technology for protecting the integrity and availability of data, telecommunications security and personal identification methods. Project updates will be exchanged quarterly, and project reviews will be provided by either party upon request of the other party.

7. Ensure the Technical Working Group reviews prior to public disclosure all matters regarding technical systems security techniques to be developed for use in protecting sensitive information in federal computer systems to ensure they are

consistent with the national security of the United States. If NIST and NSA are unable to resolve such an issue within 60 days, either agency may elect to raise the issue to the Secretary of Defense and the Secretary of Commerce. It is recognized that such an issue may be referred to the President through the NSC for resolution. No action shall be taken on such an issue until it is resolved.

8. Specify additional operational agreements in annexes to this MOU as they are agreed to by NSA and NIST.

IV. Either party may elect to terminate this MOU upon six months written notice.

This MOU is effective upon approval of both signatories.

RAYMOND G. KAMMER
Acting Director
National Institute of
Standards and Technology

DATE: Mar 24, 1989

W.O. Studeman
W. O. STUDEMAN
Vice Admiral, U.S. Navy
Director
National Security Agency

DATE: 23 March 1989

Mr. VALENTINE. Thank you, Mr. Kammer.

The level of understanding which you say is in shape to be executed by your agency and the NSA, we have seen that. I'm not going to ask you about the terms. I would just like you to comment on this phase of it.

You know, oftentimes, where there are long-lasting and inherent disagreements as to how to approach a problem, sometimes parties come to an agreement from frustration.

Is that what we have here? Or is it in your opinion a workable solution to the problems that existed from your point of view?

Mr. KAMMER. Well, the process was a long one and it was not always amicable, which is reasonable to expect. The people that I have worked with most closely on this from NSA are Dr. Jim Hearn and Admiral Studeman, both of whom will be appearing before you shortly.

Mr. VALENTINE. He just walked in.

Mr. KAMMER. They are both first-class individuals and it's been a pleasure to work with them. I have a high degree of trust in them. And I am really very confident that we're going to be able to make this work. That's probably the most fundamental part.

Whatever you write down, there's some way to think around, a way of making it not work. And it has a lot more to do with the intent of the individuals who are implementing it.

I believe the intent is there and I think it's going to work.

Mr. VALENTINE. As you well know, the international community is moving rapidly into the implementation of public key cryptography.

Will the MOU allow NIST and NSA to issue standards for public key cryptography?

Mr. KAMMER. The MOU by intent, and I believe by content, doesn't limit the authority of NIST to recommend for promulgation any concept to the Secretary of Commerce, including private key. It identifies a procedure in the rare event where it appears to NSA, not to us, that there may be some security implication that has to be taken into account; it gives the NSA an opportunity to have their opinion heard in an appropriate way.

Specifically with respect to public key, unfortunately, we left the attachment to my testimony, starting on page 6. We begin to speak of what we believe are the future issues we should address.

On the last paragraph of page 8, listed among them is public key as one of the items that we really believe is appropriate to address.

In fact, NSA, in the person of Dr. Hearn, and I have agreed that public key concepts will be first issued. And that will be addressed under the MOU.

Mr. VALENTINE. Assuming OMB issues a call for updated security plans next year, how will you approach the review process and what changes, if any, would you make?

Mr. KAMMER. I don't really know yet. I'm going to ask Mr. Burrows to comment a bit more on it. But, when we finish the review of the first 1,500 or so in June, we'll hold our lessons learned, if you will, workshop in July. And I think we can give you a more intelligent answer.

But I'll ask Jim to see if he can give you a more responsive answer than I can.

Mr. BURROWS. I believe that one of the things we have to do in the future is to get at least in some parts of the plan, probably not all of them but a few among the important ones, a look at the more detailed plan and actually what you're doing in order to implement the plan. I think that's part of what has to be looked at in the future.

In addition, I believe that we ought to ask them, in areas where they are connected to networking, how they're handling security in that area. When you discover things, like people who are using a network said they needed a secure network, and the people who are supplying a network saying nobody on that network needed security.

So it's an interesting phenomenon that's occurred. There's a disconnect some place. We have to make sure that those don't endanger security.

Mr. VALENTINE. You requested $3.5 million additional funding, according to your statement, to respond more completely to the requirements of the Act.

Could you tell us what activities, what you would do with this money? Also, how much was originally requested by the National Computer Systems Laboratory?

Mr. KAMMER. The base of the program in FY-88 was a million dollars. We requested and received a million/five. Our current base is $2.5 million. In the FY-90 budget, it includes another $3.5 million. That would bring the total program to $6 million, which is, in fact, the dollar amount that I identified in testimony prior to the passage of the Computer Security Act as the estimated cost of the program.

Remarkably enough, Mr. Plager was saying earlier, that OMB has been a strong supporter. Due to the priorities in the Commerce budget process, our original proposal to OMB was a bit short of the amount that brought us to $6 million. And OMB raised it.

This is a very unusual case but we are asking for more from Congress than we asked for from OMB and it is the dollar amount that Jim initially proposed to me. So we think it's an appropriate amount.

Mr. VALENTINE. How well in your opinion have the federal agencies identified sensitive systems operated on their behalf by States, by contractors and other organizations?

Mr. KAMMER. Some have; 10-15 percent of the 1,500 or so plans that we have have identified treated systems that are operated on their behalf by others, either private or State.

That's clearly not all of them. It is enough for us to get some experience in the review process and learn more about it.

But one expects that more will have to be done in that area in the next couple of rounds.

Mr. VALENTINE. Thank you, Mr. Kammer.

Mr. Lewis.

Mr. LEWIS. Mr. Kammer, what is the working relationship between NIST and NSA?

Mr. KAMMER. We have been cooperating very effectively on review of these plans, which is a difficult task and somewhat unstructured. So it requires a lot of good will on all sides.

In addition to that, historically we've had a good working relationship. Our first major product, if you will, in the computer security area was the Data Encryption Standard. That was produced and issued by us in the form of an Information Processing Standard, based on advice and assistance from NSA.

The history has been a good one. As I mentioned earlier, working our way through the review wasn't always perfect, but I'm very optimistic about the future and I feel like the present is good, too.

Mr. LEWIS. What do you estimate is the cost of complying with the Computer Security Act?

Mr. KAMMER. The cost for NIST, we expect $6 million a year will be an adequate program. The cost in the agencies, if you will, the owners of the federal data bases, is an unknown number to me right now. I don't think it exists. It is not going to be negligible.

Like Mr. Plager, I would argue that the cost of not implementing far exceeds the cost of implementing.

The immediate issue that people think of, of course, is disclosure of information. They say, "Well, non-federal data is disclosed." I suspect that a far more important issue is the integrity of the data has not been altered, and the implications of altered data have almost no limit in terms of the consequences, if it isn't handled properly.

Mr. LEWIS. Are you planning on using NSA inputs into your system?

Mr. KAMMER. Yes, sir. The illusion in my testimony to trust in systems is, in fact, a reference to the NSA rainbow series, if you will, which probably speaks to a most appropriate set of concerns. That's in our program plan. It's desired by NSA.

Mr. LEWIS. Following my colleague from Kansas, Mr. Glickman's concerns, do you think that the Computer Security Act, as written as being applied by various agencies that we're overseeing and looking at, do you feel we're going to be able to make this Act work? Or are we going to get bogged down in so much paperwork and regulations that we don't really have anything but a paper tiger?

Mr. KAMMER. I believe it can be made to work. I believe it will be. The reason is there's a real problem here. The people who are responsible for these systems, when they come to appreciate the problem, simply by virtue of knowing the problem exists and understanding, are going to be motivated to cure themselves. They're going to want to do it.

When you're in a situation where you have to order people to do something, you have to watch them like a hawk to make them do it through a number of bureaucracies usually. But when you have a situation where the consequences are pretty obvious and they're pretty unattractive, then the people on the scene will want to fix it.

And if we're offering advice and assistance, it makes it easier, I think they will do it. So I believe it will work.

Mr. LEWIS. I certainly hope so.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Walgren follows:]

OPENING REMARKS BY THE HONORABLE DOUG WALGREN (D-PA) ON THE JOINT HEARING ON THE IMPLEMENTATION OF THE COMPUTER SECURITY ACT OF 1987 (P.L. 100-235)

March 21, 1989

TODAY'S HEARING REVIEWS PROGRESS DURING THE FIRST YEAR UNDER THE COMPUTER SECURITY ACT OF 1987 (P.L. 100-235) AND UNDERLINES THE IMPORTANCE BOTH SUBCOMMITTEES PRESENT TODAY PLACE ON THE SUCCESSFUL IMPLEMENTATION OF THIS ACT.

COMPUTER SECURITY AND VIOLATIONS OF IT CONTINUE TO BE AN ISSUE IN THE FOREFRONT OF THE NEWS. LAST NOVEMBER, YOU MAY RECALL, THE INTERNET CLUSTER WAS THE VICTIM OF A COMPUTER VIRUS THAT PLAYED HAVOC AND STALLED COMPUTERS THROUGHOUT THE COUNTRY. THIS VIRUS, BASICALLY A PRANK, WAS THE CREATION OF A TWENTY-THREE YEAR OLD COMPUTER SCIENCE GRADUATE STUDENT. JUST LAST MONTH, THREE WEST GERMAN COMPUTER HACKERS WERE ARRESTED FOR HAVING ALLEGEDLY STOLEN UNCLASSIFIED INFORMATION ABOUT NUCLEAR WEAPONS AND COMPUTER CHIPS FROM VARIOUS U.S. GOVERNMENT DATA BASES AND PASSING THE MATERIAL ON TO THE KGB. EMBEZZLEMENT OF GOVERNMENT FUNDS BY COMPUTER CONTINUES TO BE A PROBLEM.

TO PROTECT AGAINST THESE TYPES OF INTRUSIONS, OUR TWO SUBCOMMITTEES WERE THE FIRST TO APPROVE THE LEGISLATION WHICH BECAME PUBLIC LAW 100-235. THIS LAW WAS ALSO CONGRESS' RESPONSE TO AN UNWISE WHITE HOUSE DIRECTIVE THAT 1) CREATED A NEW CATEGORY OF GOVERNMENT- CONTROLLED INFORMATION - "SENSITIVE BUT UNCLASSIFIED," AND 2) GAVE THE NATIONAL SECURITY AGENCY THE JOB OF PROTECTING COMPUTER SECURITY.

CONGRESS WAS UNWILLING TO GIVE A TOP SECRET MILITARY AGENCY CONTROL OVER THE OPERATING RULES FOR THE MANY CIVILIAN GOVERNMENT COMPUTERS WHICH AFFECT ALMOST EVERY ASPECT OF OUR LIVES INCLUDING THE BANKING SYSTEM, GOVERNMENT PENSIONS AND PAYMENTS, TAX RECORDS, AND GOVERNMENT CONTRACTS. P.L. 100-235 PLACED THE RESPONSIBILITY OF CARRYING OUT COMPUTER SECURITY FOR UNCLASSIFIED DATA IN THE HANDS OF THE CIVILIAN NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, WHILE MAKING THE GREAT EXPERTISE IN SECURITY MATTERS OF THE NATIONAL SECURITY AGENCY AVAILABLE AS NEEDED. THE ACT ALSO REQUIRED PERIODIC REPORTS TO CONGRESS ON THE PROGRESS OF THE IMPLEMENTATION OF THE VARIOUS PROVISIONS OF THE COMPUTER SECURITY ACT.

WE REALIZE THAT THE FEDERAL GOVERNMENT'S SECURITY PROGRAM HAS EXPERIENCED GROWING PAINS. A YEAR AFTER ENACTMENT OF THE LAW, THE NATIONAL SECURITY AGENCY AND THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY APPEAR

TO BE COOPERATING, BUT A FORMAL MEMORANDUM OF UNDERSTANDING WAS NOT SIGNED UNTIL A COUPLE DAYS AGO. MOST FEDERAL AGENCIES HAVE SUBMITTED THE OVER TWO THOUSAND PLANS TO PROTECT COMPUTER SYSTEMS THAT THE ACT REQUIRES. IN ADDITION, THE COMPUTER SECURITY BUSINESS IS FLOURISHING IN THE PRIVATE SECTOR, AS INFORMATION MANAGERS ARE LOOKING FOR WAYS TO PROTECT THEIR SYSTEMS AND CONSULTANTS ARE BUSY ADVISING THEIR CLIENTS ON AN EXPANDING ARRAY OF EQUIPMENT AND SOFTWARE PROTECTION.

ALL OF THE AGENCIES WITH LEAD RESPONSIBILITIES UNDER THE ACT, THE OFFICE OF MANAGEMENT AND BUDGET, THE NATIONAL SECURITY AGENCY, THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, THE OFFICE OF PERSONNEL MANAGEMENT, THE GENERAL SERVICES ADMINISTRATION, AND THE GOVERNMENT ACCOUNTING OFFICE ARE REPRESENTED HERE TODAY. WE LOOK FORWARD TO THEIR TESTIMONY. WE HOPE THE PUBLIC AIRING OF PROGRESS TO DATE WILL LEAD TO A BETTER UNDERSTANDING OF THE PROBLEMS FACED BY THOSE TRANSLATING OUR WORDS INTO ACTION AND TO AN IDENTIFICATION OF ANY SUCH PROBLEMS WHICH HAVE A LEGISLATIVE SOLUTION.

Mr. WALGREN (PRESIDING): The Chair recognizes the gentleman from Kansas.

Mr. GLICKMAN. Just a couple of quick questions, Mr. Kammer.

Tell me again what is the projected date of the signing of a Memorandum of Understanding between you and NSA?

Mr. KAMMER. I only needed the permission of my Secretary to sign it. I was content with it when I recommended it to the Secretary. I have that permission.

Admiral Studeman can give you his answer, but I know it's very soon. This week is a reasonable expectation.

Mr. GLICKMAN. Okay. You've also reported that, in fiscal year 1990, you will prepare guidance on protecting computers from virus attacks. Is that correct?

Mr. KAMMER. Yes, sir.

Mr. GLICKMAN. Is that from domestic as well as international incursions? It knows no boundaries at all?

Mr. KAMMER. No boundaries.

Mr. GLICKMAN. In addition, as you look down the road over the next 10 years, what new kinds of infections or nefarious activities do you see that will, in fact, interfere with information contained in the data bases?

We have viruses that came up in the last two or three years. You had hackers. And of course you've always had the criminal element insiders.

What else is there? New use of microwaves that can bombard computer systems? I just want to make sure we are preparing ourselves for a variety of eventualities in which folks can destroy computers or information contained there.

Is there anything that is out there? The electro-magnetic fields? Rocks? I don't know. What do we have?

Mr. KAMMER. I'm going to ask Mr. Burrows to comment on that. Unfortunately, the limits are the limits of human imagination.

Mr. GLICKMAN. Are you seeing anything new?

Mr. KAMMER. Mr. Burrows will comment.

Mr. BURROWS. I guess most of the things that have hit the newspapers in the last two years have been around for at least 10. We don't see anything new coming. The only thing new that I can think of is a determined threat from the people who want to hurt the infrastructure of an organization. That is, terrorists. That's a motivation, not a mechanism.

Mr. GLICKMAN. Right now, you don't see any new kinds of offensive technologies that could be used?

Mr. BURROWS. Offensive technologies, no. Almost all the offensive technologies, there are some that are possible, but they just cost too much. As you mentioned, attacking machines with a ray kind of activity, it looks like it would cost too much.

Mr. GLICKMAN. Could a charged particle beam or some perhaps spinoffs of the Strategic Defense Initiative?

Mr. BURROWS. If those things will melt an object several thousand miles away, they will certainly melt a computer. There are lots of easier ways to take out a computer.

[Laughter.]

Mr. GLICKMAN. Thank you, Mr. Chairman.

Mr. WALGREN. Thank you, Mr. Glickman.

The Chair recognizes the gentle lady from Maryland, Mrs. Morella.

Ms. **Morella**. Thank you. It's always a pleasure to have representatives of NIST here today. I want to thank you, Mr. Kammer, for the hard work you've done so successfully, and Mr. Burrows.

I'm curious. On page 9 of your testimony, you mentioned that the current fiscal year you have redirected $200,000 to start-up in an effort to coordinate responses to computer security incidents. And you created an information clearing house.

Could you elaborate on that? Do you want to coordinate responses to computer security, the incidents? And then, I'm also curious about what is this information clearing house?

Mr. **Kammer**. As I was saying earlier, the number of different attacks that are imaginable is very large and the way in which the attacks could be introduced is also almost limitless. You find yourself in a position where you just can't anticipate everything, especially with a civilian civil data system. Part of its functionality is the ability for people to access it and to manipulate the data, to use it.

One of the concepts that was initially proposed by the Department of Defense and has been endorsed by us, and in fact we've agreed to be major participants in it, is to identify entities in the United States who are expert in certain technologies that represent certain kinds of attack or certain kinds of defense to systems.

If a problem does arise, those are the people who will call the shots, who will give advice on how to cope with the problem that's come up.

The other aspect that we worry about, very quickly, is how do I know that the cure I'm being given is a cure rather than a poison pill?

Part of this activity is to create procedures that will allow you as the proprietor of the data system to be assured that you have just be given a cure rather than a Trojan horse or the like.

This is the nature of the activity.

Ms. **Morella**. So you're going to try to identify these so-called experts in security remedies and whatever and put them in your Roladex?

Mr. **Kammer**. Pretty much. I can see Mr. Burrows thinks I've over-simplified the answer and he's going to help.

Mr. **Burrows**. Well, it turns out, when you look at a virus attack of the kind that we recently had, it was both detected and solved by experts who were sitting on the network that was under attack. And I think that's going to be true in almost all the cases where things are attacked.

You have to understand the system in order to see that it's malfunctioning and you have to understand the system in order to understand how it's being attacked.

And outside experts can talk about it in theory, but they can't identify the specific problem that you have. And so each network or community of users is going to have to have its own reaction center which sits and watches.

And since that community manages that network in the first place, they normally do that in-house. They're sitting there watching. So they're the people that are going to have to be the first line of defense.

Ms. **Morella**. You'll be the coordinator?

Mr. **Burrows**. We will be sitting back. We and NSA will be playing the roles of assisting and watching and coordinating, yes.

But not being the front line troops.

Ms. **Morella**. You're like information in referral?

Mr. **Burrows**. Information referral and special experts, but not specific experts in that network because that is being run and managed by a different group of people who can change it daily.

Ms. **Morella**. Do you see continued funding necessary?

Mr. **Burrows**. We see that this would be a good thing. It isn't currently in our work plan, but it could end up being a big thing. And it's going to be sometime before we get all of the technology into the field which is required to avoid this kind of attack.

Ms. **Morella**. Have you taken a look at what other countries do in this particular area? Are we sort of ahead of all of them? What is that top security?

Mr. **Burrows**. We're usually the first people to see something happen and we're probably the first people to take action against it, but it is happening elsewhere.

Ms. **Morella**. But you are saying, no, we don't know what they're doing?

Mr. **Burrows**. I know what the unclassified people do, but I don't know what the classified people are doing in other countries. They are worrying the same way we are. And they're doing almost exactly the same kinds of things that we're trying to do.

Ms. **Morella**. So they're not ahead of us though, you're saying? There's not much we can gain from them at this point?

Mr. **Burrows**. No. I think we have more global networks than they do. So we're clearly capable of being attacked from more places.

Ms. **Morella**. Thank you, Mr. Chairman.

Mr. **Walgren**. Thank you, Mrs. Morella.

The gentleman from California, Mr. Rohrabacher.

Mr. **Rohrabacher**. I'll pass. Thank you.

Mr. **Walgren**. All right. On behalf of the Committee, we want to express our appreciation for your testimony. I, too, will pass and we'll hopefully get on through this hearing in some good fashion.

Thank you very much for being a resource to us. Instinctively, this area has tremendous importance and I appreciate your approaching it in the way that you have and your expressed recognition of that.

Thank you very much.

We then return to Vice Admiral Studeman, who is Director of the National Security Agency, accompanied by Dr. James Hearn, Deputy Director for Information Security.

Gentlemen, welcome to the Committee. We appreciate your being here. Your written statements will be made part of the record. You can feel free to focus on parts of the statement that you've anticipated giving the Committee, or emphasize ideas that you'd like to underscore in any way you'd like.

We'd want another introduction to the record Admiral and Mr. Hearn.

Admiral **Studeman**. This is Mr. Pat Gallagher, head of the National Computer Security Center.

Mr. **Walgren**. I'll recognize you then, Admiral. Please proceed.

STATEMENT OF VICE ADMIRAL W. O. STUDEMAN, U.S. NAVY, DIRECTOR, NATIONAL SECURITY AGENCY; ACCOMPANIED BY DR. JAMES J. HEARN, DEPUTY DIRECTOR FOR INFORMATION SECURITY; AND PATRICK R. GALLAGHER, JR., DIRECTOR, NATIONAL COMPUTER SECURITY CENTER

Vice Admiral **Studeman**. Thank you, sir. I want to apologize for coming in late. I can now report to you that we have a Secretary of Defense. I just came from his swearing in ceremony, so at least progress should be made over at Defense.

I came in time to basically monitor most of the sessions with Mr. Kammer. I believe most of the critical issues that you are interested in were answered by him. One of the advantages of coming late is that I don't have to repeat.

I would agree with him that we're only a matter of hours, if not days, away from signing the Memorandum of Agreement.

The Memorandum of Agreement I think is an important step in recognizing the shared cooperative responsibility on the part of NIST and NSA. And as you're also aware, efforts are also being undertaken to have an NSDD-like structure in effect which should probably evolve sometime in the next several months as a fully-agreed to Executive Branch document.

I think at this point in time, rather than going over the individual parts of my statement, I'm prepared to turn to your specific questions for the National Security Agency.

[The prepared statement of Admiral Studeman follows:]

56

STATEMENT OF VADM W. O. STUDEMAN,

DIRECTOR
NATIONAL SECURITY AGENCY
BEFORE THE
SUBCOMMITTEES ON TRANSPORTATION, AVIATION AND MATERIALS
AND
SCIENCE, RESEARCH AND TECHNOLOGY
OF THE COMMITTEE ON SCIENCE, SPACE AND TECHNOLOGY
OF THE HOUSE OF REPRESENTATIVES OF THE UNITED STATES
ON IMPLEMENTATION OF THE COMPUTER SECURITY ACT OF 1987
21 MARCH 1989

Mr. Chairman and Members of the Subcommittees:

I am pleased to have another opportunity to appear before you to provide an update on the progress the National Security Agency (NSA) has made in implementation of the Computer Security Act of 1987 (PL 100-235) since we testified last September. I indicated at that time our firm resolve to continue to work with the National Institute of Standards and Technology (NIST) in this area.

At the last hearing, I committed to seek a Memorandum of Understanding with NIST. I am pleased to report that as a result of much dedicated work on the part of both agencies, NSA and NIST have reached agreement at the agency level on a Memorandum of Understanding (MOU) that will enable us to move forward further in implementing our respective responsibilities under the Computer Security Act. Of particular significance is the establishment within the executive branch of a coordinated review process to address, at a very early stage and in a timely manner, national security concerns that may arise from activities intended to result in the development of security standards, techniques, and technology to protect unclassified but sensitive information. At the last hearing we also informed you that NSA would take the lead in drafting a revised version of NSDD-145. We had already begun drafting a revision to bring the NSDD into conformance with the Computer Security Act, when in January of this year we received formal direction from the National Security Advisor. That effort is proceeding; the NSA/NIST MOU is an integral step in the process.

PL 100-235 directs that NSA and NIST review annually the computer security plans of federal agencies covered by this law. We began that process in January 1989. Both NSA and NIST have allocated personnel to coordinate and manage the review, and have expended a great deal of effort in helping the agencies to develop their plans. Two workshops were held to educate more than 700 agency representatives on how to develop security plans for their computer systems. We will hold a separate workshop at the end of this month to discuss the OMB data call for 1990, and one in July to discuss experiences with the computer security planning process. Thus far we have received over 1500 computer security plans from 57 agencies and have reviewed about half of the plans.

Generally, we are encouraged by the efforts of many of those who have responded: but both NSA and NIST agree that there is a need for coordinated oversight of security plans within each participating agency. Various inconsistencies among the plans has made analysis time consuming. Preliminary review of the plans indicates that many agencies are inconsistent in their internal computer security planning processes. Frequently, computer security plans from one component of an agency cite agency security policies, directives, and guidance while another component of the same agency cites no reference in its computer security plan. Likewise, there has been inconsistency in responsiveness to the OMB call for plans (OMB Bulletin 88-16), as well as in the overall quality of the plans themselves. We are advising the agencies to focus attention on correcting these inconsistencies.

I have several examples to give you an idea of the types of advice and comments we are providing to the agencies:

When a plan provides conflicting information, we bring this to the attention of the originator, and advise the agency of the problems these conflicts can cause. For instance, one plan identified the confidentiality and integrity of information to be the primary security concerns, yet indicated that the security control measures corresponding to those concerns were not applicable. In this and similar cases, we advise the agency to reconsider the applicable control measures, cite potentially applicable laws, policies, and directives, and point out the availability of NIST and NSA publications that could be helpful in structuring the plan.

Similarly, when we encounter plans that reflect absolutely no awareness of laws, policy, or directives applicable to the security of a system, we point out the general applicability of the Computer Security Act to executive departments, the appropriate Federal Information Processing Standards (FIPS) and National Computer Security Center publications, and additional guidance that might be available from other government sources.

Some of the plans have projected the implementation of security control measures without identifying implementation dates. In these cases, we note the omission of the dates, and advise the agency that without dates it is impossible for the review team to correlate the agency's implementation priorities with the plan's primary, secondary, and minimal concerns.

Both NSA and NIST are working effectively as a team to give advice and assistance to the agencies on these plans. This joint effort is proceeding well and we hope to complete all reviews by fall 1989.

NSA's submission is one of these 1500 security plans. Our unclassified system is DOCKMASTER, the National Computer Security Center's computer system that serves as a focal point for exchanging computer security information, computer security criteria, and security product information. The system also provides electronic mail, conference support, computer security tool applications, and is used to support product evaluation teams. There are more than 2500 computer security professionals using DOCKMASTER. These users include the DoD, the Military Services, the Intelligence Community, other federal agencies, and the private sector. DOCKMASTER is currently operating at a B2 level of trust, which means that the hardware and software provide users with substantial data protection through such security features as authentication, access controls, and auditing. In addition to the internal trust features of the system, DOCKMASTER is operated in accordance with our own strict security procedures. Other security features, such as external identification and authentication of users, are also provided; user activity is continually audited. DOCKMASTER is a good model of computer system security.

The following are snapshots of various joint NSA/NIST accomplishments since last September, including actions taken in the area of computer viruses:

Last October, NIST and NCSC hosted the largest National Computer Security Conference since its inception 12 years ago. Congressman McMillen was the keynote speaker and almost 2,000 people attended.

NSA/NIST cooperated again in the aftermath of the November 1988 INTERNET computer virus. The virus seriously impacted the availability of over 6,000 computers, but greatly heightened public awareness of the perilous consequences of malicious software. It also made clear to government officials and private industry and academia the need to apply combined expertise. NSA and NIST were co-hosts for a virus symposium on 8 November. This represented not only a very timely initiative, but also an unprecedented action by responsible computer security experts, throughout the computer security community, to work as one in solving this national problem.

Let me now offer more detail about the virus problem and ongoing efforts to provide solutions. Until November of last year, it was perceived that the virus problem was largely confined to personal computers (PCs). However, the INTERNET virus attack of 2 November changed that perception by demonstrating a person's capability to impact a huge number of major host computer systems connected to one of the largest computer networks in the world. In response, a group of senior DoD officials met on 14 November as an "Executive After Action Assessment Team" to review the events of 2 November and develop recommendations for improving the Department's ability to respond to future malicious software attacks. As a result of that meeting, the Secretary of Defense tasked NSA to develop a course of action to respond to four specific tasks.

1. work with NIST and DARPA to quickly address the establishment of a central coordination center;

2. publicize computer security "lessons learned" from this incident;

3. reassess the major defense data networks on a "priority basis to determine current vulnerabilities"; and

4. pursue intensive research and development with the objective of identifying means to counter computer viruses.

Today there are no known solutions that can guarantee protection of a system against malicious software. We believe strongly that the proper use of trusted products, coupled with sound system security management and increased funding and emphasis in the area of research and development, offers the best hope for preventing, detecting, and containing such attacks. Consequently, we will continue to encourage computer security research, as well as promote the development of trusted technology by U.S. computer manufacturers and the acquisition and proper use of such products by customer organizations in the DoD and Intelligence Community. We are cooperating with DARPA to implement a high-assurance trusted system whose underlying functional capabilities are similar to those of the untrusted systems exploited in the 2 November attack.

Even when there is widespread availability and use of trusted products, diligent system and network management will continue to be the principal means upon which the DoD can rely to reduce the risk of attack. Such "common sense" operational procedures as effective password management, proper software configuration management, and aggressive user security awareness programs go a long way toward minimizing risk. Fortunately, many DoD operational systems have already taken steps in this direction, some as a direct result of the INTERNET virus. We encourage system managers, and accrediting authorities in particular, to continue to insist that such procedures are adopted and followed since the responsibility for security ultimately falls on their shoulders.

The following highlights the major points of our response to the Secretary of Defense tasking on computer viruses:

a. We are working with NIST, DARPA, DCA, the FBI, academia, and industry to improve the federal government's ability to respond to computer attacks. All parties agree that a distributed confederation of coordination facilities, rather than a single national response center, is the best approach. This strategy, founded on the principle that individual system and network managers are the first line of defense, features community response centers to assist system managers in identifying and responding to COMPUSEC problems. The national organizations identified above will be involved primarily with top-level planning, providing guidance to the community centers, and assisting individual communities when requested. NSA will make available to all participants the communications and information exchange facilities of our unclassified DOCKMASTER system, and will establish links with U.S. computer vendors to help identify and correct COMPUSEC vulnerabilities.

BEST AVAILABLE COPY

b. We have taken several steps to heighten computer security awareness in the aftermath of the 2 November incident. First, the proceedings of the 8 November post mortem were issued on 20 November and given wide distribution. Second, in cooperation with NIST and U.S. industry, we sponsored a UNIX Vendors Conference on 2 December 1988, laying the basis for wider government/industry cooperation to address computer security problems. Finally, we will issue three publications that respond to the Secretary's call for increased COMPUSEC awareness. This month, we will distribute a report that discusses viruses and some of the available software techniques for detecting them. In June, we will issue two publications, one on the role of trusted technology in combating malicious software, the other on helping system managers and security officers better use available security mechanisms and features.

c. Lastly, we will expand our current COMPUSEC R&D program to help DoD components to more effectively prevent, detect, and contain the effects of viruses and other forms of malicious software. In close cooperation with NIST, the Services, DCA, and DIA, and with input from DARPA, we are developing initiatives in four fundamental research areas: (1) software engineering of trusted computer systems; (2) formal system development methods; (3) secure operating systems; and (4) malicious software analysis tools. By focusing intensely on malicous software, we intend to develop more general techniques to replace the ad hoc approaches we rely on today.

d. By the end of 1990, we expect to have 75 products on the Evaluated Products List, which should go a long way toward providing greater protection against a large class of viruses.

EST AVAILABLE COPY

We are also optimistic about our research efforts to help reduce the time required to evaluate products at the B1 level of trust, and below. Interest on the part of computer vendors continues to increase; vendors understand in particular the marketing benefits of trusted technology. We are also enthusiastic about our research and development efforts that will aid the transfer of technology between the U. S. Government and industry. This will allow U.S. ADP manufacturers to produce trusted products, at the high-rated levels, faster and at less expense to the manufacturer. These breakthroughs may come as early as the end of 1990.

In closing, I would like to highlight, for the record, specific goals and accomplishments of the National Computer Security Center since its formation in 1981. The Center provides a base within the Department of Defense and, indeed the entire Federal Government, upon which to examine the difficult technical issues involved in computer security. Today it has established contact with virtually all U.S. computer manufacturers to encourage the development of trusted computer systems for customer installations. A primary goal of the Center is to promote the availability of off-the-shelf trusted computer systems. These are systems that employ sufficient hardware and software integrity measures for simultaneously processing a range of sensitive or classified information. Our Evaluated Product List (EPL) catalogs these products for all users interested in protecting their vital information to whatever level of protection they need.

The aim of the EPL is to provide ADP system developers, managers, and users an authoritative evaluation of a system's suitability for use in processing sensitive information. Currently, virtually every major manufacturer of computer

EST AVAILABLE COPY

systems is working with the Center in the development of trusted computer security products, with the ultimate goal of reaching a successful evaluation of its product and placement on the EPL.

While our objective is to ensure the availability of trusted products primarily for the DoD, we believe that most computer security problems are common to all environments, and that trusted products should and can be widely used. As a result, one of our aims is to try to reduce the costs of building trusted systems by encouraging demand. By so doing, we hope to eliminate the need to design and build costly one-of-a-kind systems which have not been developed with solid security principles in mind. We believe this strategy is necessary because the DoD represents only 4.8% of the world-wide revenues and 9.5% of the total U.S. ADP revenues. The DoD alone cannot provide a large enough market share to motivate cost-effective production of trusted systems at all levels.

Equally important to the advancement of U.S. computer security is providing technical guidance to DoD and others on a wide range of topics. Our program develops computer security guidance for developers, vendors, evaluators, and users of trusted products. Our most familiar guidance comes in the form of a multi-colored set of publications, generally referred to as "The Rainbow Series", consisting of such booklets as:

- The Trusted Computer System Evaluation Criteria (The Orange Book)
- The Trusted Network Interpretation Guideline (The Red Book)
- The Password Management Guideline (The Green Book)

EST AVAILABLE COPY

- **The Guideline for Applying the Trusted Computer System Evlauation Criteria in Specific Environments (The Yellow Book)**

Technical guidelines published in 1988 include implementation guidance on the subject of audit, discretionary access control, and configuration management, plus publications on design documentation, trusted facilities, and trusted distribution. Approximately 40 other guidelines are either under development or planned. All of these publications are unclassified and are available to the general public.

The Center also maintains a very aggressive research and development program that strives to achieve timely and significant breakthroughs in computer security technology. We are meeting this objective by concentrating on: secure architectures, secure database management systems, and secure networking approaches. The Center also funds an aggressive program for verification and evaluation research to support the development of new architectural approaches and products.

Once again, I thank you for the invitation to testify before your Subcommittees. If you have any questions, I would be pleased to entertain them now.

Mr. WALGREN. All right. Do any of the other gentlemen have any prepared testimony?

Dr. HEARN. No, I do not.

Mr. GALLAGHER. No.

Mr. WALGREN. Okay. As you know, the international community is moving quickly in implementing public key cryptography. Will the Memorandum of Understanding allow NIST with NSA's direction to issue standards for public key cryptography?

Dr. HEARN. The MOU that is about to exist between our two agencies provides for a review process. It provides for a working group to look at technical issues like that, Mr. Chairman.

As Mr. Kammer testified, one of the first issues that we'll be working on together is the idea of international standards for public key systems.

Mr. WALGREN. How does any rewriting of the National Security Decision Directive 145 conform with the Memorandum of Understanding that you anticipate?

Are we rewriting NSDD 145?

Admiral STUDEMAN. There is an Executive level type document that is being written. It's not actually an NSDD. It is currently in staffing. In effect, the approach being used is the same approach that's being used in the MOU. It focuses basically on enhancing the process that allows the discussion to take place on the National Security side and on the NIST Commerce side and provides for the structure whereby the National Security side and the interests of the law that are pursued for unclassified but sensitive and public sector enhancing of computer systems can be basically pursued in trains.

So basically it allows us to have a process whereby that maximum level of dialogue can take place starting with the kinds of things that are already elaborated in the Memorandum of Agreement now with technical working groups and parallel sorts of structures that take us all the way up through the system, in case there is some kind of difference of opinion about which way we ought to go.

Mr. WALGREN. And you expect to have this memorandum with NIST signed in the near future? Is there a target date for that? I apologize. I'm coming in late.

Admiral STUDEMAN. Yes. As Mr. Kammer told you, the Secretary of Commerce has already approved on the NIST Commerce side. We have one last step in coordination with Defense with OSD/C3I guidance. We anticipate we'll get their approval any hour now, so we should be able to sign this document with Defense and Commerce both having concurred in it sometime in the next several days at the most.

Mr. WALGREN. Let me apologize for not being here earlier and not having as deep a background in this area as I should. But, how would you characterize the memorandum that you anticipate signing?

What are the most important aspects of it to you as an NSA person responsible for the National Security Administration?

Vice Admiral STUDEMAN. To me, the most important aspect of the draft Memorandum of Agreement we anticipate signing is really to provide the vehicles whereby the communications and the participation can take place on a dual track, basically.

NSA, to fulfill its interests on the national security side for federal computer systems to protect classified information and for NIST and Commerce to basically pursue the track that is their responsibility under the law on unclassified but sensitive—perhaps there's some confusion in terminology, but it perhaps serves best to describe what we're talking about—and the piece of the legislation which also discusses the activities in the public sector.

So it provides the structure whereby we can communicate and participate together with technical working groups to identify early on the standards, the guidelines and the kinds of technical issues that needed to be pursued in order to ensure that we are able to secure the kinds of computer systems that the law addresses.

Mr. WALGREN. What do you envision in a financial sense of the commitment of NSA under this agreement and in the area generally?

Vice Admiral STUDEMAN. I'm not going to describe the full size and scope of the NSA's budget because, basically, that's a classified number, but the size of our budget is substantially larger than the size of NIST's budget. And we've had a significant investment in the area of computer security.

And if you look at communications security as a subset adjunct of computer security, obviously, that investment over the years both in terms of people and dollars is very large.

So, in the context of the nature of the Center, the nature of the series of things that have been pursued both in terms of technology, R&D, the development of standards, the development of guidelines, the nature of the dialogue, not only with NIST but with others in government, and the nature of the dialogue with industry to pursue the issue of enhanced communications and computer security, that budget has been translated into a large computer center and lots of other, if you will, specific activities.

Perhaps Dr. Hearn or Pat Gallagher would like to elaborate a little bit on some of the specific things that those NSA dollars basically buy.

Mr. WALGREN. We'd appreciate that for the record.

Mr. GALLAGHER. The program that we have been embarked on since 1981 is one that has attempted to do a number of different things. One is to stimulate the computer industry in the United States, to get them to create trusted technology.

To the extent that trusted technology will be applicable across-the-board for most of the applications that we saw, where we and the government could benefit from some of that, and the rest of the population could also benefit from some of that, because we believe, as was mentioned by Mr. Glickman earlier, we believe that we should have some concern for other systems than the National Security systems for which protection was created.

So we have created this system that encourages American industry to bring to the Center products to be evaluated, products that are main line computer products that would be available as just common items for people to select from.

By the end of FY-90, as is in the Admiral's testimony, we will have 75 products on our list, products from the main stream of

American industry. That's a very labor-intensive effort to do evaluations.

We've also created publications, as was mentioned earlier by Mr. Kammer. Our Rainbow Series of publications, the orange books and red books and that kind of thing, specify what it is that we mean by trusted technology and how one should use it.

We've had a vigorous research and development program for quite some time that pursues five areas—architectures, how our machines are built and how should they be built. Networks, what does it mean by the connecting of machines together and what might we say about those networks. Data bases because data bases, as has already been mentioned here this afternoon, are very complex, very important. Verification technology, which is very esoteric study of how it is that you prove exhaustively that you have what you believe you have.

And then aids to evaluation, how may we automate the tools which allow us to do the evaluation that we do.

As the Admiral mentioned, also because we have included communications security, we create some very special products for use within the Defense community, which combined both the aspects of communications security and computer security. And that, in general, is what we have been up to over the last year or so.

Mr. **Walgren**. Dr. Hearn, do you want to add to that?

Dr. **Hearn**. No, I don't have anything to add to that.

Mr. **Walgren**. We're not used to panels where people don't have anything to add.

[Laughter.]

Mr. **Walgren**. But it's appropriate, I'm sure, in your line of work.

[Laughter.]

Mr. **Walgren**. I guess what was going through my mind was remembering the offer that the NSA was originally in the position of making, that they wanted to operate very broadly in this whole area.

We've sort of tried to draw some lines where there is very appropriate dominance in one area but, at the same time, one of the reasons NSA made the offer is because they have resources, and resources can be secured to support the security function for the country.

They cannot be secured to support the commercial function for the country. We would like to see you continuing to provide the kind of support and interest that you would have had you had the whole responsibility.

Certainly, the interest and the support of research efforts that seemed to make sense, even though we're involving NIST in a very broad range of line responsibility.

Vice Admiral **Studeman**. I would like to say that history I think has been generally an excellent history. Whatever differences we've had I think quite honestly have been on the margin, although they're frequently important differences.

But, in the context of NIST and NSA specific past relationships and current and future relationships, I'm extremely optimistic about the outlook. I think that if past models serve as any example, that there has been a significant amount of cross-over representing NSA's technical and fiscal strength and our pursuit of technology in the area that you've already mentioned.

A great deal of cooperation, even in the past whereby NSA's capabilities have basically crossed over into the national interest and have had application for the unclassified but sensitive and public sector applications, not the least of which of course is the digital encryption standard activities that we've undertaken over the last couple of years.

Mr. WALGREN. Maybe you could have somebody at this point in the record respond to the specific question of what are NSA's near-term plans for continued support of NIST with respect to—the suggestion is the computer network security, but my instinct would be to ask you to respond to that question perhaps in the four areas or the five areas that you've set out. So we have something for the record specifically of what your near-term plans are for the support of NIST.

Vice Admiral STUDEMAN. We'd be happy to provide that in writing, sir.

[The material referred to follows:]

NATIONAL SECURITY AGENCY NEAR-TERM PLANS FOR SUPPORT TO THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY IN THE AREA OF RESEARCH AND DEVELOPMENT

As mentioned at the September 1988 hearing of your committee on implementation of the Computer Security Act of 1987, NSA provided NIST a detailed accounting of our computer security activities, which included the ongoing education, training, and awareness efforts at NSA; an annotated bibliography of our completed technical guidelines, those currently being written and those planned; information on interoperability standards and functional profiles; and a list of suggested research and technical topics to be briefed to NIST to aid in developing needed standards. We also released two communications security protocols derived from NSA's Secure Data Network System (SDNS) program for incorporation in the Government Open System Interconnection Profile (GOSIP).

Since that time, NSA has briefed NIST personnel on the Low-cost Encryption/Authentication Device (LEAD) program, currently being developed under an NSA no-cost contract. In conjunction with the LEAD discussions, NSA has held technical interchanges with NIST in the areas of personal data security, authentication, data integrity, and data confidentiality.

We have spoken to NIST to determine which of the five research areas require immediate assistance, and they have expressed primary interest in the following three. We plan to hold monthly meetings with NIST to ensure that they receive the assistance they require:

1. Architecture: This includes near-term interest in a new hardware-based architectural approach to building trusted systems (LOCK), and an update on the recent 24-month demonstration of the LOCK development.

2. Networks: NIST is interested in communications security protocols from NSA's Secure Data Network System (SDNS) program, and has developed its own interoperability testbed using the output of three SDNS contractors. These NSA contractors have demonstrated working examples of SDNS protocols, which should aid NIST in developing standards.

3. Secure Data Base Management Systems: We will share information on our research progress.

Discussions with NIST reveal that there is little interest in both verification technology (due to the lack of short-term benefits), and automating evaluation tools, since NIST does not conduct evaluations of commercial trusted computer security products.

On 5 May, the NIST and NSA representatives to the Technical Working Group established under the NSA/NIST Memorandum of Understanding will hold their first meeting. An important objective of the first meeting will be to address and prioritize the specific needs of NIST and to develop the mechanism for responding to their requirements.

Mr. **Walgren**. Let me recognize the gentle lady from Maryland, Mrs. Morella.

Ms. **Morella**. Thank you, Mr. Chairman. I want to pick up on that point because I'm looking at a couple of different areas. One of them is to pursue intensive research and development with the objective of identifying the means to counter computer viruses.

Then, you say, But, right now, there is no known solution to this, to guarantee protection of a system against malicious software. Any comment on that and the direction in which you're going, progress which you're making and how do you go about doing it?

Vice Admiral **Studeman**. Let me start on that and turn it over to the experts, if I may. First off, I think we have to make a distinction between the systems and the government that contain classified information and systems that we're talking about that NIST will address, which are the systems that don't tend to contain classified information.

The federal computer systems that contain classified information tend to be configured differently, so that it seems to me the main threat is basically from within because you can only attack the systems generally from within.

They're not generally accessible from the outside; whereas, many of the other systems you're talking about may or may not be accessible from the outside. In particular, a lot of the discussions with regard to the things that appeared in the press recently, the Internet issue, the issue with regard to the West German hacker attack are examples of external attack. That's not to say that viruses don't cause a problem for you, even when you have control of your own system. Even we at NSA have to very carefully guard against people coming and introducing software disks or other kinds of things that can potentially have resident on them viruses which can then migrate out into the system.

This is a very difficult thing to achieve technically. However, the progress that you make in one area is translatable to the other. That is, for the classified systems and the unclassified systems, the technology can be very much the same. The standards, the guidelines that are required.

But there really is no way right now at present to guarantee against this kind of assault. And I think that's an important point to leave with the Committee, that those kinds of guarantees can't be made.

As we strive on the classified side for more and more robust trusted systems, particularly operating on a multi- level security side, we hope to be able to provide much greater, more robust, in depth safeguards against this.

But this is still a difficult thing. Perhaps Pat would like to make some additional comments.

Mr. **Gallagher**. I would agree with the Admiral that this is a tough problem in structuring how one goes about solving this very tough problem, it falls into two parts. One is that we must increase people's awareness as to what it is that they should do with the things that they now own.

That translates very simply into discipline in the computing environment. One should recognize that computers are important and the information that they possess is important, and one should treat them with some degree of respect, therefore.

For example, one should always be able to answer the question: Who has access to the machines that I am dealing with? Do I know? Do I care? What are the privileges that those people or those systems which touch me electrically, what privileges do they have?

Those are simple questions that can be answered. Sometimes, they are long because there are lots of connections. But that should be a question that everyone on a system ought to want to know.

What are the privileges that people have? What is the capacity of the system? Simple things like does the system use passwords? Are they enforced? Are there some rules? Other complex questions can be asked, but those are very simple.

So, from the standpoint of education, of making people sensitive, we are working very closely, I believe, with both NIST and OPM in trying to enhance training, educational awareness as to how you can bring discipline and an attitude toward the computing environments.

We have transferred all of the course modules that we had created within our environment to those organizations for them to use as they wished in the broader environment of the government and the private sector, and we will continue to do that.

Now, from a technology standpoint, there are other things that need to be created. They need to be created in the arena of: How do you recognize a virus? And that's really a question of:

How do you understand the behavior of the network? Is the network operating properly or not? How do viruses operate? What is their mechanism of propagation? Do we understand them well?

And the answer is: Some we do and some we don't.

Simple viruses that we had seen over the last couple of years that generally attack PCs, we understood pretty well. They left footprints. You could find their mechanism for propagation. And similarly, when we saw in the November virus, we saw a propagation mechanism, we have begun to codify what is a virus, how does it propagate, how might it propagate?

Now, there's other ways that one might want to look at this problem.

How do programmers write programs? Is this a valid program? Is there some way of wrapping it either physically or electronically so that I know that which you sent me is what you really sent me? So that it didn't have anything in there infectious. So our research then looks at both the administrative things that we would like to get people sensitive to and we share that with the broader community and a technology which we have intensively worked out to lay out and will share with a very broad community at the end of this March, to let people look at what it is that we propose to do and see if all of the bases are covered in laying out a program that gets much more intensively into the virus.

I prefer a term "malicious code", because that's a broader template.

One last example I think might help you. In the November virus, there was an attack in the send mail command. Now, lots of people who use the network like to send mail. This routine allowed for a debug in the send mail command. There is no need for a debug feature in a send mail command because you're only sending mail.

But, it was put in by the system designer when the system designer was debugging. But it was left in when that version of Unix was promulgated into the system. It violates a principle of which we are advocates, which is the principle of least privilege. No operating system, no command and no person ought to have more privileges than they need to have to do the job they need to do.

It's a fundamental principle that we believe ought to be advocated in the computer arena. It has not often been advocated in the past.

So that's a technical issue. It's a philosophical issue, and we're working both.

Ms. MORELLA. It sounds like you're talking about discipline, common sense. For a while, you sounded like you were giving a paper at a medical convention.

[Laughter.]

Ms. MORELLA. It's interesting in terms of the discipline needed for those various commands. Very interesting. I appreciate your telling us about it.

Did you want to comment, Dr. Hearn?

Dr. HEARN. No.

Ms. MORELLA. Enough is enough?

Thank you. We appreciate your keeping us posted on the progress that is being made.

Thank's, Mr. Chairman.

Mr. WALGREN. Do you get a fight on the approach of least privilege necessary as a principle? Are there people who say, Gee, it makes sense for people to be able to do more with the computer rather than less.

Mr. GALLAGHER. The best example I can give you, sir, is that when we were evaluating a vendor's Unix program to be one of those candidates for our evaluated products list, that also had, because it was a Unix program, a send mail feature in it.

When it was brought us for evaluation, the debug capability had been removed because that manufacturer recognized that it had no place under the philosophy of least privilege. So I believe that we are getting the kinds of attitudes.

But I believe they have also come slowly. People in general like to have as many privileges as they can think of, whether they need them or not.

So I think, as we look into the last decade of the century, we will find that that will be a cultural problem. The technology can be created to allow you to enforce it but the managerial responsibility will have to be insisted upon from the people who run the networks.

Vice Admiral STUDEMAN. It seems to me though that it's doctrinally agreed that this is what you need to do, it's just a question then of discipline enforcement technology procedures. And policy in individual computing environments.

Mr. WALGREN. But it just strikes me though as a first impression that that runs counter to some of the things that in some agencies I've sensed we have going on.

I've noticed in this article from the Washington Post on the 4th of March that they speak of sort of a computer democracy. The dichotomy being that, on the one hand, they want to protect the information. On the other hand, the computer creates power that essentially creates an information democracy that only unfettered computers have the power to create.

So when you really across-the-board enforce that least capability on individuals with access to computers, you limit their ability to be creative, I gather, in some ways then, perhaps.

Vice Admiral STUDEMAN. It does seem to me, however, you can't have it both ways. If you have a democracy kind of approach, and there are systems that support the democracy in computing environment, then you can't expect to have the kind of security that you would have on a system that is self-contained and executing, let's say.

It's not a sophisticated, highly-classified security environment. You cannot have democracy. For example, on the FAA's air traffic control.

Mr. WALGREN. It seems that in some instances though you might want to have—I guess we anticipate there's very strict controls over classified and sensitive information. But, in areas where you're not sensitive, perhaps this principle of least privilege is not as dominant.

Vice Admiral STUDEMAN. The art form is to develop a set of security standards that can assist at the high end of the spectrum and at the low end of the spectrum. I suspect quite honestly that that's what we've done, I think, in the basic layout we have with the hierarchical approach to computer standards.

Mr. WALGREN. Let me ask with respect to the West German incident, have we described for the record yet the kind of information that was under attack? The types of information that might have been accessed by the Soviet Union?

Vice Admiral STUDEMAN. I'm not sure what earlier speakers said, and I apologize for punting. But since this is an open case being actively investigated and pursued by the FBI, although we do know something about it tracking from a distance, I think it would probably be inappropriate for me to actually lay out and articulate the details.

Mr. WALGREN. Are there specific defenses to this that are obvious to us?

Vice Admiral STUDEMAN. This is a difficult computing environment in which to execute defenses because these are large networks that access many aspects of computing data bases within the country. So there are definitely some lessons learned here.

But I believe that the lessons learned are probably the lessons we already knew.

Mr. WALGREN. Any other contributions on that?

[No response.]

Mr. WALGREN. And then, assuming that OMB calls for updated security plans in the very near future, is that anticipated at this point? By the way, is there any indication that OMB is going to be asking much more of us in this area?

Dr. HEARN. I think it has been said earlier this afternoon that we have to finish the review process that we're embarked upon and there is going to be an interim look in a lessons learned sense, next week.

Once this experience is evaluated in some detail, then there will be a better basis to judge that. But that's more OMB's task.

Vice Admiral STUDEMAN. I think, from our point of view, we did articulate in our statement for the record the kinds of diverse, disparate responses that we've gotten back. And that we have evaluated. There are clearly some things that we have to decide with respect to where we're going to go from here in order to assure that we do this efficiently for the future, and get the end objective obtained here, which is to finally get a clear statement from the Departments and Agencies and find a way to start working with them to tighten up their systems.

Mr. WALGREN. Are there specific recommendations other than what you might have outlined in your written statement, which was part of the record, that you would be making to OMB at this point? Are there sort of themes?

I'm just exploring for what might be the ground that OMB should be covering if they ask for near-term performance in these areas.

Vice Admiral STUDEMAN. I really do think it would be premature until we've had a chance to review and consolidate and take a look through these vehicles we've described and the statements about how we're going to check where we are in the process.

I think it would probably be premature to give you an answer.

Mr. WALGREN. Is there anything else you'd like to tell us while you're here?

Vice Admiral STUDEMAN. No, sir. I would just like to reiterate again I believe that we've established a Renaissance relationship with NIST now. We're moving out together in a partnership arrangement, a shared responsibility. And I am optimistic for the future. These are not trivial issues to deal with either from a policy point of view, from a technical point of view or from the point of view of how we're going to deal with this problem in the federal government.

So, again, we look forward to reappearing before this Committee periodically to give you an update on our progress.

Mr. WALGREN. Thank you very much on behalf of both of our Committees. We want to express our appreciation to you for your cooperation and being a resource.

Thank you very much.

Let's turn then to Curtis Smith, Associate Director of Career Entry and Employee Development in the Office of Personnel Management.

We appreciate your coming to the Committee, Mr. Smith. Your written statement will be made a part of the record. Please feel free to focus on the points you would like to emphasize in any way that you would like.

STATEMENT OF MR. CURTIS J. SMITH, ASSOCIATE DIRECTOR FOR CAREER ENTRY AND EMPLOYEE DEVELOPMENT, OFFICE OF PERSONNEL MANAGEMENT

Mr. SMITH. Thank you. I will do that. I appreciate the opportunity to appear this afternoon. The Computer Security Act gave OPM one primary responsibility. That was to regulate the matter of computer security awareness training in the agencies.

We have published an interim regulation which agencies are able to use, which makes great use of NIST's guidelines. We will publish a final regulation at such time as the guidelines themselves become final, because of the close relationship between the two of them.

We didn't quit, however, with publication of the regulations, but have spent a fair amount of time creating training materials that can help agencies go about the business of enhancing the awareness of computer security in their work force—video tapes, one-day classes, a variety of things that we have made available to agencies free of charge. And we will also in our regular training program provide training to agencies if they wish us to do it.

We have looked at the GAO report on compliance with the Computer Security Act's training requirements. We see that most people thought they were well-served by our regs, but we will also work with those who didn't find them helpful and make sure the regs do as much as possible in this area.

We will also use both the GAO report and the kinds of information coming from the computer security plans to get a better sense of what is happening on the training side of the Computer Security Act.

As we get that information, we will begin to work with the agencies who may need to do more and can do more to make sure that the effort to educate keeps going.

Finally, I suppose I would say that we have gone through the process required by the Act internally as an agency that has computer systems and have found that a very constructive thing, particularly in bringing program managers to grips with the security implications of their systems.

And I think for the first time having them sit down and think through the security requirements as they went through the security planning process.

And we look forward to workshops that will follow so we can learn what others have found out about that as well.

Those I think are the points I would like to make. I'd be happy to answer questions.

[The prepared statement of Mr. Smith follows:]

Insert T.6

STATEMENT OF
CURTIS J. SMITH
ASSOCIATE DIRECTOR FOR CAREER ENTRY
AND EMPLOYEE DEVELOPMENT
OFFICE OF PERSONNEL MANAGEMENT

before the

SUBCOMMITTEE ON TRANSPORTATION, AVIATION,
AND MATERIALS AND THE SUBCOMMITTEE
ON SCIENCE, RESEARCH, AND TECHNOLOGY
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES

at a hearing on

IMPLEMENTATION OF THE COMPUTER
SECURITY ACT OF 1987

MARCH 21, 1989

MESSRS. CHAIRMEN AND MEMBERS OF THE SUBCOMMITTEES:

THANK YOU FOR ASKING ME TO APPEAR THIS AFTERNOON TO DISCUSS THE WORK THE OFFICE OF PERSONNEL MANAGEMENT HAS BEEN DOING TO CARRY OUT ITS RESPONSIBILITIES UNDER THE COMPUTER SECURITY ACT.

WHILE I AM QUITE NEW TO THIS AREA--COMPUTER SECURITY TRAINING, ALONG WITH OPM'S OTHER TRAINING ACTIVITIES, HAS ONLY COME UNDER MY ORGANIZATION SINCE YOUR LAST HEARING--I KNOW THAT YOU HAVE BEEN ENGAGING IN VERY ACTIVE OVERSIGHT OF THE WORK THE EXECUTIVE BRANCH HAS BEEN DOING TO IMPLEMENT THE PROVISIONS OF THE COMPUTER SECURITY ACT. RECENT EVENTS, SUCH AS THE INTERNET COMPUTER VIRUS INCIDENT, HAVE CERTAINLY

BROUGHT TO EVERYONE'S ATTENTION THE TREMENDOUS IMPORTANCE OF THIS WORK TO ENSURE THE SECURITY OF OUR FEDERAL COMPUTER SYSTEMS.

UNDER THE COMPUTER SECURITY ACT, OPM WAS REQUIRED TO ISSUE A REGULATION PRESCRIBING THE PROCEDURE, SCOPE, AND MANNER OF COMPUTER SECURITY TRAINING, AND THAT WAS DONE, LAST JULY. SINCE THE REGULATION MUST IMPLEMENT THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY'S TRAINING GUIDELINES, WHICH HAVE NOT YET BEEN FINALIZED, WE ISSUED AN INTERIM REGULATION, WHICH WE WILL REVISE AND REPUBLISH AS SOON AS THE GUIDELINES ARE COMPLETED. OPM DOES NOT, OF COURSE, VIEW THIS ISSUANCE OF THE REGULATION AS ENDING OUR INVOLVEMENT IN THIS PROGRAM. INSTEAD, WE HAVE BEEN ENGAGED IN A CONTINUING EFFORT TO ASSIST AGENCIES IN UNDERSTANDING AND CARRYING OUT THE NEW TRAINING REQUIREMENT. WE HAVE WORKED CLOSELY WITH THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY ON THEIR TRAINING GUIDELINES. WE HAVE SPONSORED OR PARTICIPATED IN BRIEFINGS AND SEMINARS AROUND THE COUNTRY FOR AGENCY MANAGERS AND COMPUTER SECURITY OFFICIALS TO ACQUAINT THEM WITH THEIR TRAINING RESPONSIBILITIES AND LEARN FROM THEM HOW WE CAN HELP THEM CARRY OUT THESE RESPONSIBILITIES. WE HAVE BEEN DEVELOPING EXTENSIVE TRAINING MATERIALS FOR AGENCY USE, AND WE HAVE BEGUN CONDUCTING COMPUTER SECURITY COURSES THROUGH OUR OWN TRAINING CENTERS.

IN ALL OF THESE ACTIVITIES, WE HAVE BEEN GUIDED BY THE NEED FOR FLEXIBILITY. THERE IS A GREAT DEAL OF VARIETY AMONG AGENCIES, IN THEIR MISSIONS, THEIR STRUCTURES, THEIR APPROACH TO NEW PROGRAMS, AND CONSEQUENTLY, THEIR COMPUTER SECURITY TRAINING NEEDS. AS WE HAVE MET WITH FEDERAL MANAGERS FROM DIFFERENT AGENCIES AND DIFFERENT LOCATIONS TO DISCUSS COMPUTER SECURITY TRAINING, WE HAVE BEEN STRUCK BY THE DIFFERENT SITUATIONS THEY FACE, AND WE HAVE TRIED TO BE AS FLEXIBLE AS POSSIBLE, WHILE STILL ENSURING THAT EVERY AGENCY'S COMPUTER SECURITY TRAINING WILL BE MEANINGFUL AND WILL MEET THE ACT'S GOALS.

IN REVIEWING GAO'S NEW REPORT ON COMPLIANCE WITH THE COMPUTER SECURITY ACT'S TRAINING REQUIREMENTS, WE WERE PLEASED TO SEE THAT OUR APPROACH TO THE DEVELOPMENT OF THE TRAINING REGULATION WAS VIEWED POSITIVELY BY THE AGENCIES, WITH NEARLY TWO-THIRDS OF THE RESPONDING AGENCIES SAYING THAT OUR REGULATION WAS HELPFUL TO THEM. WE CERTAINLY INTEND TO FOLLOW UP WITH GAO AND THE AGENCIES TO SEE IF WE CAN IDENTIFY THE REASONS THE OTHER AGENCIES DID NOT FIND OUR REGULATIONS HELPFUL, AND TRY TO MAKE THE RESPONSE EVEN BETTER. WE WILL ALSO CONTACT THE AGENCIES IDENTIFIED AS NOT YET HAVING STARTED TRAINING AND SEE HOW WE CAN HELP THEM GET STARTED. OVER THE LONG TERM, WE HOPE TO USE THE COMPUTER SECURITY PLANS SUBMITTED BY

AGENCIES AS A VEHICLE FOR MONITORING AGENCY TRAINING IN COMPUTER SECURITY AWARENESS.

ONE OF THE AREAS WHERE WE HAVE THOUGHT WE COULD BE MOST HELPFUL TO THE AGENCIES IN CARRYING OUT THE TRAINING REQUIRED BY OUR REGULATION IS BY PROVIDING APPROPRIATE TRAINING MATERIALS. OBVIOUSLY, IT WILL BE MUCH LESS EXPENSIVE TO THE GOVERNMENT TO IMPLEMENT THE REQUIRED TRAINING IF WE CAN AVOID HAVING EACH AGENCY HAVE TO DEVELOP ITS OWN TRAINING MATERIALS. HERE AGAIN, WE HAVE TRIED TO KEEP IN MIND THE DIFFERENT NEEDS OF DIFFERENT AGENCY ENVIRONMENTS, AND THE DIFFERENT TARGET AUDIENCES WITHIN AGENCIES. WE HAVE PREPARED A BASIC COURSE FOR A STRUCTURED TEACHING SITUATION, WITH LESSON PLANS, INSTRUCTOR'S AND PARTICIPANT'S HANDBOOKS, AND SO FORTH. FOR OTHER AUDIENCES, WE HAVE PREPARED SUCH OPTIONS AS AN EXECUTIVE BRIEFING PACKAGE AND A VIDEOTAPE, AND WILL SOON HAVE AVAILABLE AN INDEPENDENT STUDY COURSE. WE BELIEVE THE READY AVAILABILITY OF THESE TRAINING MATERIALS, WHICH HAVE ALREADY BEEN PROVIDED TO ABOUT 300 DIFFERENT GOVERNMENT ORGANIZATIONS, WILL BE VERY HELPFUL TO AGENCIES IN CARRYING OUT THE REQUIRED TRAINING. I WOULD LIKE TO SUBMIT COPIES OF THESE TRAINING MATERIALS FOR YOUR INFORMATION.

OF COURSE, AGENCIES ALSO HAVE THE OPTION OF ENROLLING THEIR EMPLOYEES IN TRAINING COURSES GIVEN BY OPM. WE ARE CONDUCTING THESE COURSES IN WASHINGTON AND AROUND THE COUNTRY, AND

EXPECT TO CONDUCT ABOUT 60 SESSIONS WITH SOME 1500 PARTICIPANTS BY THE END OF THE FISCAL YEAR. WE ARE ALSO ADDING COMPUTER SECURITY ISSUES TO SOME OF OUR OTHER TRAINING COURSES, SUCH AS OUR EXECUTIVE DEVELOPMENT COURSES. WE EXPECT ALL OF THIS ACTIVITY TO EXPAND RAPIDLY.

THE FIRST YEAR OF A NEW PROGRAM, PARTICULARLY ONE THAT EXTENDS THROUGHOUT THE FEDERAL GOVERNMENT, ALWAYS PRESENTS DIFFICULTIES, AND WE WERE QUITE PLEASED TO SEE IN THE GAO REPORT THAT, OF THE 66 AGENCIES THAT REPORTED THEY HAVE COMPUTER SYSTEMS COVERED BY THE ACT, TWO-THIRDS HAD ALREADY BEGUN THEIR TRAINING LAST YEAR, WITH MOST OF THE REST PLANNING TO START BY THIS APRIL. WE ARE GOING TO CONTINUE OUR EFFORTS TO MEET WITH AS MANY GROUPS AS WE CAN, TO SPREAD THE WORD ABOUT THE REQUIREMENT FOR COMPUTER SECURITY TRAINING, AND THE DIFFERENT WAYS TO ACCOMPLISH IT EFFECTIVELY, AND TO GET COMMENTS FROM AGENCIES ON HOW WE CAN BE MORE HELPFUL TO THEM IN FULFILLING THEIR TRAINING RESPONSIBILITIES UNDER THE ACT. WE ARE ALSO, OF COURSE, GOING TO BE WORKING CLOSELY WITH THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY TO ENSURE THAT TRAINING IS ADEQUATELY ADDRESSED IN AGENCY COMPUTER SECURITY PLANS. WE BELIEVE THAT, AT THIS POINT IN THE PROGRAM, THESE ACTIVITIES WILL GIVE US A GOOD VIEW OF THE PROGRESS THE GOVERNMENT IS MAKING.

YOU ALSO ASKED THAT I SPEAK TO OPM'S OWN EFFORTS IN IMPLEMENTING THE COMPUTER SECURITY ACT INTERNALLY. I HAVE LOOKED INTO THIS AND HAVE FOUND THAT WE ARE MAKING PROGRESS. WE HAVE COMPLETED OUR COMPUTER SECURITY PLANS, WHICH WERE SUBMITTED TO THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY FOR ADVICE AND COMMENT IN EARLY JANUARY. WE HAVE BEEN INCREASING EMPLOYEE AND MANAGERIAL AWARENESS OF COMPUTER SECURITY ISSUES THROUGH TRAINING RELATED TO SPECIFIC COMPUTER SYSTEMS, REMINDERS AND NOTICES TO EMPLOYEES ON COMPUTER SECURITY TOPICS SUCH AS VIRUSES AND PASSWORD SECURITY, AND WIDE DISTRIBUTION OF SECURITY GUIDELINES AND POLICIES, PARTICULARLY RELATING TO MICROCOMPUTERS. WE HAVE ALSO IDENTIFIED THE TARGET AUDIENCE OF EMPLOYEES--MORE THAN A FIFTH OF OPM'S WORKFORCE--TO RECEIVE THE NEW CLASSROOM TRAINING DEVELOPED IN RESPONSE TO THE COMPUTER SECURITY ACT, AND WE EXPECT TO BEGIN THIS TRAINING BY EARLY MAY.

THANK YOU. I WILL BE GLAD TO ANSWER ANY QUESTIONS THE SUBCOMMITTEES MAY HAVE.

Mr. **Walgren**. I appreciate that, Mr. Smith. When you look at OPM's own training materials, are there areas that are uncovered at this point? How do you assess the reach of OPM's present training materials?

Mr. **Smith**. I guess it's hard to know with any finality; the world in this area may be almost infinite. We've had those out not for a terribly long period of time. We're just now beginning to get reactions to them. We will pay a lot of attention to what people indicate they also need in there if it's not there.

And we are quite happy and prepared to enlarge them in whatever ways we can.

Mr. **Walgren**. Do they just go out to OPM, or do they go out to agencies other than OPM?

Mr. **Smith**. No, sir. In this case, we sent them to about 300 agency people as well.

Mr. **Walgren**. Three hundred other agency people.

Mr. **Smith**. Right.

Mr. **Walgren**. Are those OPM's own internal guidelines or teaching materials or training materials?

Mr. **Smith**. I guess the answer is both. They're the materials that OPM trainers would use, an agency called and said please come and do this computer security training for me. But also because we wanted to have the impact as wide as possible, as quickly as possible, and to make it attractive to agencies, we have given these very same materials to all of the agencies in 300 cases so they, themselves, can use them, particularly where it's something they do now in addition to other training that they were providing anyway, for example.

Mr. **Walgren**. GAO identified a number of agencies as not having started training at this point. Is that right?

Mr. **Smith**. That's correct.

Mr. **Walgren**. Your role is to contact them at some point?

Mr. **Smith**. Yes. That's what we will do. We will work through that GAO report and make calls to the people who have either not responded or have said they haven't started the training yet.

Mr. **Walgren**. When will we have an assessment of their response?

Mr. **Smith**. There are several pieces of that. I don't know that I have a date ready in mind. The first piece of it is making the contact to be sure that the people, in fact, are on track.

We also would like to begin looking through the sorts of information coming in the computer security plans. That's a longer-term project. I'm not quite sure when we would have that finished. I suspect that we will have worked through the GAO report in a matter of several weeks.

Mr. **Walgren**. We'd like to ask whether there is a method for reviewing the present security plans and whether there's a schedule for completing that review of present security plans.

I gather, of all the agencies, those who have responded or those who have started working with their people, and those who are not yet working.

Mr. **Smith**. What we had planned at this time and I assume we are talking just about the training here and not about the larger implementation plans that are going to OMB.

What we're looking to do in the first instance is to ensure that everybody is on track and getting their training underway. We have not scheduled reviews beyond that.

Mr. **Walgren**. Do you have any responsibilities beyond that in the Act?

Mr. **Smith**. Probably not because the agency heads by the Act are made explicitly responsible for doing the training. For example, they are given the authority to ignore the Act completely if they think they have a training program that's as good as the one that would be set up under OPM's regs and NIST's guidelines.

We are interested, however, that agencies take this seriously and do them well. So I wouldn't want to distance myself completely.

Mr. **Walgren**. Is there a report—I guess I should ask for a report that would make some assessment of where the agencies that have not yet started training, where they are in this process and when they will start training, I gather, and how your work with them progresses.

Mr. **Smith**. Certainly, we will do such a report just to enable us to do our own work. We'd be happy to share it with the Committee.

[The material referred to above follows:]

United States
Office of
Personnel Management
Washington, D.C. 20415

JUN 21 1989

In Reply Refer To:

Your Reference:

Honorable Doug Walgren
Chairman, Subcommittee on Science,
  Research, and Technology
Committee on Science, Space and Technology
U. S. House of Representatives
Washington, DC 20515

Dear Mr. Walgren:

In response to the request from the Committee, we have contacted the agencies identified in the GAO report, "Computer Security: Compliance with Training Requirements of the Computer Security Act of 1987," as not having started computer security awareness training.

Of the 21 agencies listed in Table I.1 as not being in compliance with the training requirement at that time, OPM now finds that 15 are delivering computer security awareness training.

Five have firm starting dates for their training program. We will check to see that they actually start as planned. One, the Civil Rights Commission, does not have training plans because they have no mainframe computer and only three personal computers in the agency. We think this is a proper decision.

AGENCIES WITH COMPUTER SECURITY TRAINING PROGRAMS

Board for International Broadcasting
Commodity Futures Trading Commission
Congressional Budget Office
Consumer Product Safety Commission
Farm Credit Administration
Federal Emergency Management Agency
Federal Energy Regulatory Commission
Federal Trade Commission
Inter-American Foundation
International Trade Commission
National Science Foundation
Office of Personnel Management
Office of Technology Assessment
Railroad Retirement Board
Securities and Exchange Commission

CON 114-24-3
January 1980

STARTING DATES FOR AGENCY PROGRAMS

June 1989
  Interstate Commerce Commission
  National Mediation Board

July 1989
  National Labor Relations Board

September 1989
  Action
  Library of Congress

If there is any further information the Committee would like, OPM is always willing to respond, and we will continue our efforts to ensure that Federal employees are made aware of the importance of computer security.

Sincerely,

Curtis J. Smith
Associate Director
for Career Entry and
Employee Development

Mr. WALGREN. Do you have any idea when we're going to reach that point?

Mr. SMITH. I would guess several weeks. If you want a more specific commitment than that—

Mr. WALGREN. No, we operate on a month by month time frame around here. If you can get us something within several weeks, we're doing good.

I certainly would appreciate it if you would keep us informed of your assessments of how these agencies are starting up their training programs—those that have not, those that do and what your assessment of how those that start to train, how effective they are.

I gather that's within your responsibility. Is that right?

Mr. SMITH. Yes. We certainly need to know those things.

Mr. WALGREN. We would appreciate being directly informed of your own internal views of that progress.

Mr. SMITH. Certainly.

Mr. WALGREN. Thank you very much, Mr. Smith. We appreciate your being available to us.

Without you, the score would be nothing/nothing. So we appreciate it.

Mr. SMITH. Thank you.

Mr. WALGREN. Let's then call the last two witnesses together, Francis McDonough, Deputy Commissioner for Federal Information Resources Management of the General Services Administration—welcome, Mr. McDonough. And, Howard Rhile, Associate Director for Information, Management and Technology Division of the General Accounting Office.

Mr. Rhile, we appreciate your joining us. Let me ask you to both give your testimony in the order in which I've introduced you to the record, so we'll start with Mr. McDonough. I do know that your written submissions will be reproduced for the record and you should certainly feel free to underscore points in the oral transcript that you would like to stand out in whatever way you'd like.

Let's start with Mr. McDonough and then we'll turn to Mr. Rhile.

Mr. McDonough.

STATEMENT OF MR. FRANCIS A. MCDONOUGH, DEPUTY COMMISSIONER FOR FEDERAL INFORMATION RESOURCES MANAGEMENT, GENERAL SERVICES ADMINISTRATION

Mr. McDONOUGH. Thank you, Mr. Chairman. I thought I would just follow up on two commitments we made to this Committee at the last set of hearings. We talked to you previously about awarding a contract which would help agencies to conduct risk assessments and physical security audits and other kinds of work they need to do relative to the Computer Security Act.

We did award that contract in 1988. I'm happy to tell you, in October 1988, and it's underway at this time.

The second thing is we published an information technology installation security/physical security. We published a good document on that in December 1988, just a few months ago. It helps agencies lay out the components of a good physical security plan, and it helps them to go on and develop that plan for themselves.

Aside from our governmentwide activities, Mr. Chairman, we are an agency, of course, which follows the Computer Security Act. We've identified 27 intense, sensitive systems in GSA in the past year; plans for those sensitive systems came in from across the agency in December and they were forwarded to NSA and NIST in January, and feedback is coming back from those agencies this week on those systems.

So, governmentwide and as an agency, we've made some interesting progress, I would say, in the six months since the last hearing.

So, if there are questions, Mr. Chairman, for the General Services Administration, I would be happy to take them.

[The prepared statement of Mr. McDonough follows:]

STATEMENT OF FRANCIS A. McDONOUGH
DEPUTY COMMISSIONER
OFFICE OF FEDERAL INFORMATION RESOURCES MANAGEMENT, GSA

BEFORE THE
SUBCOMMITTEE ON TRANSPORTATION, AVIATION, AND MATERIALS
AND
SUBCOMMITTEE ON SCIENCE, RESEARCH AND TECHNOLOGY
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

MARCH 21, 1989

Good afternoon Mr. Chairman and members of the subcommittees. The General Services Administration (GSA) appreciates the opportunity to testify again on this important issue. The Computer Security Act of 1987 was timely and very much needed to provide direction for the Federal government.

In our governmentwide role, GSA provides leadership across the government in Federal Information Resources Management in several ways. Regulations, implementing Congressional legislation, are provided through the Federal Information Resources Management Regulation (FIRMR) system. GSA, provides an extensive series of guidelines, bulletins, handbooks, and self inspection reference documents to all agencies to help them to implement the regulations and legislation. Finally, assistance is provided to agencies. This takes the form of direct, person-to-person assistance through our Agency Liaison Officer program; and, assistance is provided through a series of optional-use contract schedules programs through which specialized skills and services are made available to Federal agencies at reduced prices and in a timely manner.

To help implement the Computer Security Act of 1987, GSA will employ the Federal Information Resources Management Regulation (FIRMR) System. GSA will assist the Office of Management and Budget in the planning process. Finally, specialized assistance will be provided to agencies. Let me address first how GSA will use its FIRMR regulatory system to implement the provisions of the legislation.

GSA plays an important and essential role in implementing within the Federal Government the computer security standards developed by the National Institute of Standards and Technology (NIST). The Federal Information Resources Management Regulations (FIRMR) system, managed by GSA, requires Federal agencies to use NIST standards in the management and use of information technology resources. In addition, the FIRMR requires Federal contracting officers to include NIST standards in solicitations for information technology resources. These key FIRMR policies will apply to computer security standards when standards are published by NIST.

As individual computer security standards are published, GSA will work with NIST and Federal agencies, and the information technology industry to develop contract clauses that are consistent with the applicability criteria in the standards for contracting officers to use in specifying the standards in Federal contracts.

In addition, GSA has emphasized the emerging importance of standards through the publication of the "ADP and Telecommunications Standards Index". This document is a part of the FIRMR system. It provides Federal agencies with a complete reference document on current NIST standards and related contract clauses. As computer security standards are published by NIST, GSA will update the "ADP and Telecommunications Standards Index" to ensure agencies have a complete, up-to-date and easy-to-use reference document.

The legislation establishes a requirement for agencies to develop individual security plans for systems containing sensitive information and to incorporate summaries of these plans in the agency's five-year information systems plan. GSA will continue to assist OMB in developing the annual, five-year plan for the government.

With regard to GSA plans to provide assistance to agencies it is important to point out that we have a history of providing assistance to agencies in addressing Security issues. For example, a contract for security risk analysis was first awarded on September 18, 1984. One hundred task orders for risk analysis services were placed against this contract by Federal agencies before the contract expired on January 18, 1989.

Because of increased Federal interest in information security created by Public Law 100-235 and GSA's desire to ensure consistent implementation of the security services provided, GSA management determined that the best approach for the continued provision of these much needed security services would be to award a new single contract with nationwide coverage. This contract was awarded to an 8a firm, COMSIS, in October, 1988.

Under this nationwide contract the contractor will make available a number of security services, including (1) Risk Analysis, (2) Contingency and Disaster Recovery Plans, (3) Security Test and Evaluation Plans, (4) Physical Security Audits, (5) Sensitive and Criticality Assessments, and (6) Security Training Awareness Courses. These services will be available to Federal agencies on a non-mandatory basis by entering into interagency agreements with GSA. The contract is not intended to be all encompassing or the only avenue of support to Federal agencies needing assistance in the security area. It is intended to supplement rather than supplant agencies' independent efforts to acquire such services.

GSA will ensure the quality of services rendered under this contract. Our goal is to provide uniform and consistent assistance to agencies in implementing the security requirements mandated by Federal law and regulation. In order that Federal agencies may remain abreast of the latest development in the security arena, the contractor will maintain an electronic bulletin board that client agencies will be able to access for the latest security advisories and guidance.

To complement the services that will be available under the nationwide security services contract, a publication entitled "Information Technology Installation Security" was published in December, 1988. This document will assist agency managers to define and implement physical security programs in Government facilities which handle sensitive information.

The publication defines the components of a security program and provides procedures for developing, implementing, and maintaining a practical and effective physical security program that:

> Complies with laws, policies, regulation, standards, and guidelines influencing or directing security policy; and

Provides reasonable assurance that assets are protected from potential risks and threats.

All of GSA's activities in providing assistance to agencies will be conducted in accordance with the guidelines and standards issued by NIST.

In addition to GSA's governmentwide responsibilities, GSA is implementing the Security Act within the agency itself as are all other Federal agencies. A Computer Security Awareness Training program has been developed and is being implemented. Two other categories of actions are underway.

1. Identifying sensitive systems.

   Implementing procedures were issued under a GSA order dated October 26, 1987. These identify and validate GSA sensitive systems and require:

   - A description of the criteria to be employed in determining if a system is sensitive;

   - A requirement that all sensitive systems are included in the agency's 5-Year IRM Plan, including the date of the last sensitivity evaluation;

- Procedures for evaluating the security controls of sensitive systems (covering personnel management, physical and environmental conditions, operations and transactions, and output, data storage and backup/recovery controls);
- Procedures for certifying that sensitive systems are secure;
- Appointment of a security officer in every GSA office to ensure compliance with security policy and directives and to provide agency-level liaison and coordination; and
- An IRMS review of GSA systems and associated certifications to ensure that sensitive systems are appropriately identified and certified.

A call was issued to the Heads of GSA Services and Staff Offices (HSSOs) requiring identification and certification of sensitive systems. GSA has identified 27 sensitive systems. These systems include the Personnel Information Resources System, National Electronic Accounting and Reporting System, Payroll Information

Processing System, FSS-19 Supply System, and the PBS Information System, Investigations Information System. All sensitive systems are identified as such in the 5-Year Plan. IRMS has reviewed these systems for certification compliance. Each GSA office has appointed a security official with responsibility for coordinating the requirements of the Computer Security Act.

2. Submitting Security Plans.

Letters were sent to the HSSOs transmitting OMB Bulletin 88-16 and requiring the preparation of the required security plans. All plans were received by mid December 1988. GSA formally transmitted these plans on January 5, 1989 in compliance with the OMB Bulletin. A GSA contractor is currently:

- evaluating how well the GSA procedures address the Security Act;
- evaluating how well the procedures are being followed;
- reviewing the quality of the security plans; and

- providing recommendations on possible improvements to the GSA Computer Security Program

Mr. Chairman, I would like to thank you for the opportunity to discuss all of the actions GSA is taking to help implement the Computer Security Act of 1987. We are serious about our responsibilities to help protect the data which the American people entrust to the computer systems of the Federal government.

Mr. **Walgren**. Thank you, Mr. McDonough.
Mr. Rhile.

STATEMENT OF MR. HOWARD G. RHILE, JR., ASSOCIATE DIRECTOR, INFORMATION MANAGEMENT AND TECHNOLOGY DIVISION, GENERAL ACCOUNTING OFFICE; ACCOMPANIED BY MR. DAVID GILL

Mr. **Rhile**. I appreciate the opportunity to testify today, Mr. Chairman. My prepared statement summarizes the results of questionnaires for federal agency implementation of the Act to training and security plan requirements, our work on related assignments to ascertain methodologies used by 10 federal agencies in identifying the extent of the systems operated by other organizations, and GAO's own response to our questionnaire on compliance with the security requirements for the Act.

I appreciate your offer to allow me to highlight that statement now. I'd first like to highlight information on the agency's responses regarding their computer security training programs.

As you know, the Act requires that within 60 days of the issuance of training regulations by OPM, federal agencies must start training in computer security awareness.

OPM's training regulation was issued on July 13, 1988. Therefore, the training programs had to be in place by September 11th. The chart which is before you shows the responses to a questionnaire that we mailed to 85 agencies.

I must point out that we have not independently verified that information.

Mr. **Walgren**. Is that chart part of your written testimony as well, so that the Committee has it?

Mr. **Rhile**. Yes, sir, it is. Briefly, between October 12th and December 12, 1988, we received the following responses from these 85 agencies. Forty-five or about 53 percent reporting having started the required training program in compliance with the Act. Nineteen agencies, or about 22 percent, reported that they planned to start training programs between November '88 and April 1989.

So, about 75 percent of the agencies by the end of April should have the training programs in place according to their responses to our questionnaire. Two agencies said that they had not started the training program and didn't tell us when they would start such training.

Fifteen agencies said that they had no computer systems with sensitive information. And four agencies as of December 12th did not respond to our questionnaire. We've had a flurry of response activities in the last week or so; all four of those have now responded.

Now, the full results of our training questionnaire are contained in our February report.

With your permission, I would like to also place that in the record of this hearing.

[The material referred to follows:]

GAO

United States
General Accounting Office
Washington, D.C. 20548

Information Management and
Technology Division

B-231257

February 22, 1989

The Honorable John Conyers, Jr.
Chairman, Committee on
  Government Operations
House of Representatives

The Honorable Robert A. Roe
Chairman, Committee on Science,
  Space, and Technology
House of Representatives

In your February 23, 1988, letter you requested that we determine whether federal agencies are complying with provisions of the Computer Security Act of 1987. As agreed with your offices, our three-part effort uses questionnaires to determine compliance with specific requirements and milestones of the act.

Our first report[1] provided the status of (1) agencies' compliance with the requirement to identify their federal computer systems containing sensitive information as defined by the act, and (2) Office of Personnel Management's (OPM) compliance with the requirement to issue training regulations on computer security training. This second report addresses agencies' compliance with the requirement to start training programs in accordance with OPM's training regulation. A third report will address agencies' compliance with the requirement to submit, by January 8, 1989, security plans for each of their federal computer systems containing sensitive information.

For this report, we sent a questionnaire to the 85 federal agencies not specifically exempted from compliance with the act. As discussed with your offices, we did not independently verify their responses. Appendix I describes our objectives, scope, and methodology.

The Computer Security Act (P.L. 100-235), enacted January 8, 1988, provides for improving the security and privacy of sensitive information in federal computer systems. Section 5(a) of the act requires periodic training in computer security awareness and accepted computer security practice for all employees who are involved with the management, use, or operation of each federal computer system containing sensitive information within or under the supervision of that agency. Under section 5(b), training must start within 60 days of the issuance of the OPM training regulation required in section 5(c). OPM issued its interim training regulation on July 13, 1988.

---

[1] Computer Security: Status of Compliance With the Computer Security Act [illegible] (GAO/IMTEC-88-61BR, Sept. 22, 1988).

On December 12, 1988, we briefed the requesting offices on the status of federal agencies' compliance with sections 5(a) and 5(b). Appendix I summarizes that information.

Many agencies have taken action to comply with sections 5(a) and 5(b) of the act. Of the 81 agencies that responded to our questionnaire between October 12 and December 12, 1988:

- 45 reported having started computer security training programs as required by the act.
- 19 reported plans to start the required training programs during the period November 1988 through April 1989.
- 2 reported having none of the required training programs and did not say when they would start. These two agencies were the Commission on Civil Rights and the National Mediation Board.
- 15 stated they have no computer systems containing sensitive information. Four agencies responded differently to the previous questionnaire. The Board for International Broadcasting and Federal Energy Regulatory Commission previously reported no sensitive systems; however, in response to our second questionnaire, they reported sensitive systems. The Commission on the Bicentennial of the U.S. Constitution and the Federal Labor Relations Authority previously reported they had at least one sensitive system, but now report having no sensitive systems.

Four agencies did not respond to our questionnaire. Two of these agencies, the Environmental Protection Agency and Federal Election Commission, reported having computer systems containing sensitive information in response to our previous questionnaire. The Advisory Council on Historic Preservation previously reported having no sensitive systems and the National Security Council did not respond to our previous questionnaire.

Appendix II contains our questionnaire, while appendix III details the agencies' computer security training courses and course modules.

This report was prepared under the direction of Howard G. Rhile, Associate Director. Other major contributors are listed in appendix IV.

Agency comments were not obtained because of the number of agencies involved.

Ralph V. Carlone

Ralph V. Carlone
Assistant Comptroller General

Mr. **Rhile**. The second part of our testimony is on the agency's compliance with the actual requirements to submit computer security plans to NIST.

We sent a questionnaire again to the same 85 agencies in January and February of this year—the chart before you. We've received responses from about 80 percent of these agencies so far.

This chart before you now shows the responses that we received from those agencies; 42 agencies or about half, 49 percent, reported they had submitted all their security plans to NIST by January 8, 1989, as required by the Act; 14 agencies said that they did not submit some or all of their security plans to NIST by January 8th. Most of these said that they would have them submitted by August of this year.

Twelve agencies reported that they didn't have any sensitive systems, and 17 agencies had not yet responded to the questionnaire.

I might add that nine of those have since responded. Now, more details of the agencies' responses are in my prepared statement.

I'd like to turn now to the third part of our testimony today, our work on the related assignment. As requested by the Committees on Government Operations and Science, Space, and Technology, we contacted 10 federal agencies to determine the methodologies that they used to identify sensitive systems operated by other organizations such as contractors, other federal agencies or State and Local governments.

As you know, on November 29th, the Committees themselves requested these 10 agencies to provide lists of such systems and this chart here shows the number of sensitive systems that were reported to the Committees by the 10 agencies and as updated for us, when we went to visit the 10 agencies.

As you can see, they reported a total of 121 systems operated by contractors. None of them reported systems operated by State or local governments. And two departments, Agriculture and Defense, did not include systems from all of their components.

As you can see on the chart, the Department of Energy did not report the number of systems as requested by the Committee. I understand, however, that Energy did provide a list last week. I have not had a chance to look at that list.

In talking to the 10 agencies, or in doing our work for this assignment, three of them expressed some concerns about difficulties in implementing the Computer Security Act. For example, Agriculture told us, and, indeed, reported to the Committee, that State data processing systems that support Food Stamps, for example, cannot be identified as federal systems, in part, because food stamp processing is apt to be a relatively minor part of the total processing of the State systems.

Ag, the Department of Agriculture, however, is developing security standards which I think are currently with OMB for approval. And if approved it will be mandatory for States participating in their program.

HHS also didn't identify any systems that are operated by State or local governments. They said that State systems are not federal computer systems because they're not operated by the federal government.

One official expressed concern over the amount of research and time that would be necessary to provide an accurate list of State and local systems that receive federal funds and that the Department would not attempt such an effort unless required to do so.

This concludes my statement, Mr. Chairman.

[The prepared statement of Mr. Rhile follows:]

United States General Accounting Office

GAO **Testimony**

For Release
on Delivery
Expected at
2:00 p.m. EST
Tuesday
March 21, 1989

STATUS OF COMPLIANCE WITH THE COMPUTER SECURITY ACT OF 1987

STATEMENT OF
HOWARD G. RHILE, ASSOCIATE DIRECTOR
INFORMATION MANAGEMENT AND TECHNOLOGY DIVISION

BEFORE THE
SUBCOMMITTEE ON TRANSPORTATION, AVIATION, AND MATERIALS
SUBCOMMITTEE ON SCIENCE, RESEARCH, AND TECHNOLOGY
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

Mr. Chairmen and Members of the Subcommittees:

We appreciate the opportunity to testify today on federal agencies' implementation of the Computer Security Act of 1987. As you know, at the request of the Chairmen of the House Science, Space, and Technology Committee and the House Government Operations Committee, we are conducting a three-part effort to determine whether federal agencies are complying with the specific requirements of the act.

As requested, my prepared statement today summarizes the results of questionnaires on federal agencies' implementation of the act's training and security plan requirements, our work on a related assignment to ascertain the methodologies used by ten federal agencies in identifying their sensitive systems operated by other organizations, and the General Accounting Office's response to our questionnaire on compliance with security plan requirements of the act.

AGENCIES COMPUTER SECURITY TRAINING PROGRAMS

I would first like to summarize information on agencies' responses regarding their computer security training programs. As you know, the Computer Security Act of 1987 requires that within 60 days of the issuance of a training regulation by the Office of Personnel Management (OPM), federal agencies must start training in computer security awareness and accepted computer security practices. The training is for all employees involved with the management, use, or operation of federal computer systems containing sensitive information within or under the supervision of the agencies. OPM's training regulation was issued on July 13, 1988, and agencies' training programs were to be in place by September 11, 1988.

As discussed in our recent report,[1] we sent a questionnaire to 85 federal agencies[2]. Our objectives were to ascertain whether the agencies had started the required training, obtain information on their computer security training programs, and ascertain their satisfaction with guidance provided by the National Institute of Standards and Technology (NIST) and OPM.

Chart 1 (attached) shows the responses to the questionnaire mailed to the 85 agencies to ascertain whether they had started training programs as required by the act. I must point out that, as discussed with your offices, we did not independently verify the information in the agencies' responses. Between October 12, 1988, and December 12, 1988, we received the following responses:

---

[1] Computer Security: Compliance With Training Requirements of the Computer Security Act of 1987 (GAO/IMTEC-89-16BR, February 22, 1989).

[2] These are the same agencies to which we sent our questionnaire on compliance with training requirements of the act. Our report, Computer Security: Compliance With Training Requirements of the Computer Security Act of 1987 (GAO/IMTEC-89-16BR, February 22, 1989), explains the universe of 85 agencies.

- 45 agencies (53 percent) reported having started the required training program.

- 19 agencies (22 percent) reported that they plan to start training programs, and will start them during the period from November 1988 through April 1989.

- 2 agencies (2 percent)--the U.S. Commission on Civil Rights and the National Mediation Board--reported they had not started the required training program, and did not indicate when they would start such training.

- 15 agencies (18 percent) stated that they have no computer systems with sensitive information.

- 4 agencies (5 percent) did not respond as of December 12, 1988. Three of these subsequently responded. The Advisory Council on Historic Preservation said that the Council had no sensitive systems. EPA reported that it has had a training program in place since June 1987, and that its training program includes three classroom courses or modules and six nonclassroom activities. The National Security Council (NSC) reported that all computers operated by or on behalf of NSC are protected at least at the top secret level. As of March 8, 1989, attempts to obtain a response from the Federal Election Commission had been unsuccessful.

Agencies' Responses Concerning Training Activities

In response to our questionnaire, agencies also provided information on the types of activities in their training programs. Details are in our February 1989 report.

- Thirty-one of the 45 agencies that reported having started training programs identified a total of 190 classroom courses or modules.

- Thirty-five of the 45 agencies that have training programs reported a total of 114 nonclassroom training activities.

- The responding agencies were generally satisfied with guidance provided in NIST's draft training guidelines and OPM's training regulation.

MANY AGENCIES HAVE SUBMITTED THE REQUIRED SECURITY PLANS

The second part of my testimony today is on the agencies' responses to our questionnaire to determine their compliance with the act's requirement to submit computer security plans to NIST. In our questionnaire, we asked (1) whether the agencies submitted security plans to NIST by January 8, 1989, (2) the number of security plans and systems and the organizations that operate them, (3) the criteria used to assess risk and develop protection requirements, and (4) agencies' satisfaction with OMB's guidance for preparing security plans. In January and early February, we sent our questionnaire to 85 federal agencies. As of March 6, 1989, we had received responses from 68[3] of the 85 agencies.

The Computer Security Act of 1987 requires that, within one year of enactment, each federal agency establish a plan for the security and privacy of each federal computer system containing sensitive information. The plans should be commensurate with the risk and magnitude of harm that would result from the loss, misuse, or unauthorized access to or modification of the information contained in the system.

Chart 2 (attached) shows the responses of 85 agencies on the submission of computer security plans to NIST as required by the act. Again, we did not independently verify the information in the agencies' responses. As of March 6, 1989, in response to our questionnaire:

- 42 agencies (49 percent) reported that they submitted security plans to NIST by January 8, 1989, as required by the act.

---

[3] Department of Defense submitted a consolidated response for the four defense agencies to which we sent a questionnaire. The agencies are the Departments of Air Force, Army, Defense, and Navy.

- 14 agencies (17 percent) reported that they did not submit all of their security plans to NIST by January 8, 1989. Twelve of these said they had either done so by January 13, 1989, or would do so by August 11, 1989. The agencies are the Departments of the Air Force, Army, Commerce, Defense, Interior, Justice, Navy, and Transportation; Federal Election Commission; Interstate Commerce Commission; Securities and Exchange Commission; and Congressional Budget Office. The Executive Office of the President did not specify when it would submit its plans to NIST. The remaining agency, the Federal Reserve Board, reported that it did not submit its security plan to NIST because it is not a federal agency as defined in the act.

- 12 agencies (14 percent) reported that they did not have sensitive systems as defined in the act. These agencies are the Administrative Conference of the U.S., African Development Foundation, American Battle Monuments Commission, Central Intelligence Agency, U.S. Commission on Civil Rights, Committee for the Purchase from the Blind and Severely Handicapped, Federal Mediation and Conciliation Service, Foreign Claims Settlement Commission, National Commission on Libraries and Information, National Security Council, National Transportation Safety Board, and Postal Rate Commission. One of these agencies, the U.S. Commission on Civil Rights, in responding to our previous questionnaires, reported that it had sensitive systems.

- 17 agencies (20 percent) had not yet responded to the questionnaire. These are the Departments of Agriculture and Labor; ACTION; Advisory Council on Historic Preservation; Board for International Broadcasting; Commission on the Bicentennial of the U.S. Constitution; Commission of Fine Arts; Copyright Royalty Tribunal; Environmental Protection Agency; Inter-American Foundation; Joint Financial Management Improvement Program; Library of Congress; National Credit Union Administration; Office of Personnel Management; Office of Technology Assessment; Smithsonian Institution; and U.S. Information Agency.

Number of Security Plans Submitted to NIST by Operator

As of March 6, 1989, 54 agencies reported the number of security plans by operators of the systems. Because many of the agencies reported systems in more than one category, the number of agencies adds up to more than 54. I would like to note that Defense indicated that it expects to submit several thousand more plans to NIST by August 11, 1989.

- 48 agencies reported 1,172 plans covering 2,245 systems they operate. The Departments of Defense, Energy and State reported 77, 18, and 15 security plans, respectively, but did not identify the number of systems covered by their plans.

- 11 agencies submitted 19 plans covering 19 systems operated by other federal agencies.

- 16 agencies submitted 184 security plans covering 228 systems operated by contractors. The Departments of Defense and Energy submitted 3 and 70 plans, respectively, covering systems operated by contractors, but did not identify the number of sensitive systems covered by the plans.

- 1 agency, the Department of Education, reported a plan for one system operated by a state or local government.

Criteria Used To Assess The Risks To Sensitive Systems

The 54 agencies also reported the criteria they used to assess risks to sensitive systems. Because several agencies reported using more than one criterion to assess risks and develop protection requirements for their sensitive systems, the number of agencies totals more than 54.

- 27 agencies reported that they used either OMB Circular A-123, A-130, and or the Computer Security Act to assess risks and to develop protection requirements for their sensitive systems.

- 4 agencies used formal risk analyses independent of A-123 and A-130, but did not provide details of their criteria.

- 30 agencies reported other means of assessing risk. Of these 30 agencies, seven reported that they used internal agency guidance to assess risk and eight reported that they used informal risk assessments to determine the risks to their sensitive systems. For example, the Department of the Treasury reported that it used audits, management reviews, and informal management assessments to identify risks and to develop protection requirements.

Agencies Are Satisfied With OMB Guidance

Of the 52 agencies that responded to our questions regarding their use of OMB's guidance on developing security plans (OMB Bulletin 88-16, dated July 6, 1988 and a September 6, 1988, memorandum containing answers to commonly asked questions about the act), 38 (73 percent) were either satisfied or very satisfied with OMB guidance. Forty-six (88 percent) believed that OMB's guidance was helpful in preparing their security plans.

IDENTIFICATION OF SENSITIVE SYSTEMS OPERATED BY OTHERS

I would now like to turn to the third part of our testimony today, our work on a related assignment. As requested by the Committees on Government Operations and Science, Space, and Technology, we contacted 10 federal agencies to ascertain the methodologies they used to identify sensitive systems operated by other organizations, such as contractors, other federal agencies, or state and local governments. As you know, on November 29, 1988, the Committees requested the ten agencies to provide lists of sensitive computer systems operated by other organizations on their behalf. The agencies were asked to respond to the Committees by January 9, 1989. The ten agencies are the Departments of Agriculture, Defense, Energy, Health and Human Services, Interior, Justice, Labor, and Treasury; and the National Aeronautics and Space Administration and Environmental Protection Agency.

I will briefly summarize the (1) number of systems each agency reported, including updates provided to us; (2) general methodology used by the agencies to identify sensitive systems operated by others; and (3) concerns expressed by the agencies in implementing the Computer Security Act of 1987.

Number of Systems Reported

Chart 3 (attached) shows the sensitive systems operated by other organizations that were reported to the Committees by the ten agencies. The numbers on the chart reflect updates that were provided to us by the agencies. As you can see, the ten agencies reported a total of 121 systems operated by contractors. None of the agencies reported systems operated by state or local governments. Two departments'--Agriculture and Defense--reports did not include systems from all of their agencies. And the

Department of Energy did not report the number of systems as requested by the Committees.

Methodologies Used to Identify Systems

We obtained a description of the methodologies used by the ten agencies to identify for the Committees their sensitive systems operated by others. We contacted the headquarters and one main component at each of the ten agencies.

Generally, the agencies' headquarters requested that their main organizational components identify sensitive computer systems operated by other organizations. Some agencies sent a copy of the Computer Security Act or definitions of terms along with their reporting instructions. The agencies' headquarters consolidated the information they received and prepared an agency response. Some agencies used computer security plans, inventories, or other documentation as a check to ensure the lists submitted to the Committees were complete.

Concerns Expressed By Agencies

Officials of three of the ten agencies expressed some concerns about difficulties in implementing the Computer Security Act.

- The ADP Security Officer, Office of Information Resources Management, Department of Agriculture told us and reported to the Committee on Science, Space, and Technology that States' data processing systems that support food stamps cannot be identified as federal systems, in part, because food stamp processing is apt to be a relatively minor part of the total processing on the states' systems. The official also reported that the department, together with the Department of Health and Human Services, has developed security standards which, if approved, will be mandatory for States participating in their programs.

- The Acting Director, Information Resources Management, Department of Health and Human Services, stated that HHS did not identify any systems that are operated by state or local governments. He said that state systems are not federal computer systems because they are not operated by the federal government. The official expressed concern over the amount of research and time that would be necessary to provide an accurate list of state or local systems that receive federal funds. The official added that such an effort would be a large undertaking and the department would not attempt such an effort unless required to do so.

- The Assistant Director, Office of Information Resource Management, Department of the Treasury, stated that Treasury contacted NIST to find out what constitutes a sensitive system.

The official said that Treasury has other concerns and will be working with NIST to obtain further clarification of the act.

GENERAL ACCOUNTING OFFICE'S RESPONSE TO SECURITY PLAN QUESTIONNAIRE

The fourth part of our testimony today summarizes the General Accounting Office's (GAO) response to a questionnaire that we sent to 85 federal agencies regarding compliance with security plan requirements of the act. In our questionnaire, we asked (1) whether security plans were submitted to NIST by January 8, 1989, (2) the number of security plans and systems by operator, (3) the criteria used to assess risk and develop protection requirements, and (4) satisfaction with OMB's guidance for preparing security plans.

In its response to our questionnaire, GAO stated that it

- submitted its security plans to NIST by January 8, 1989.

- submitted a total of 11 security plans to NIST covering 11 computer systems. Five plans are for systems operated by GAO, four plans are for systems operated by other federal agencies for GAO, and two plans cover systems operated by contractors.

- performed vulnerability analyses, which included formal site surveys, in accordance with guidance contained in OMB Circular A-

130 and the Computer Security Act to verify levels of risk and establish procedures for protecting sensitive information.

- was satisfied with OMB guidance on preparing security plans and believes the guidance was helpful in preparing its security plans.

-   \-   \-   \-

This concludes my prepared statement. I will be pleased to respond to any questions that you or others may have at this time.

CHART 1

GAO

Compliance with Training Requirements, as of December 12, 1988

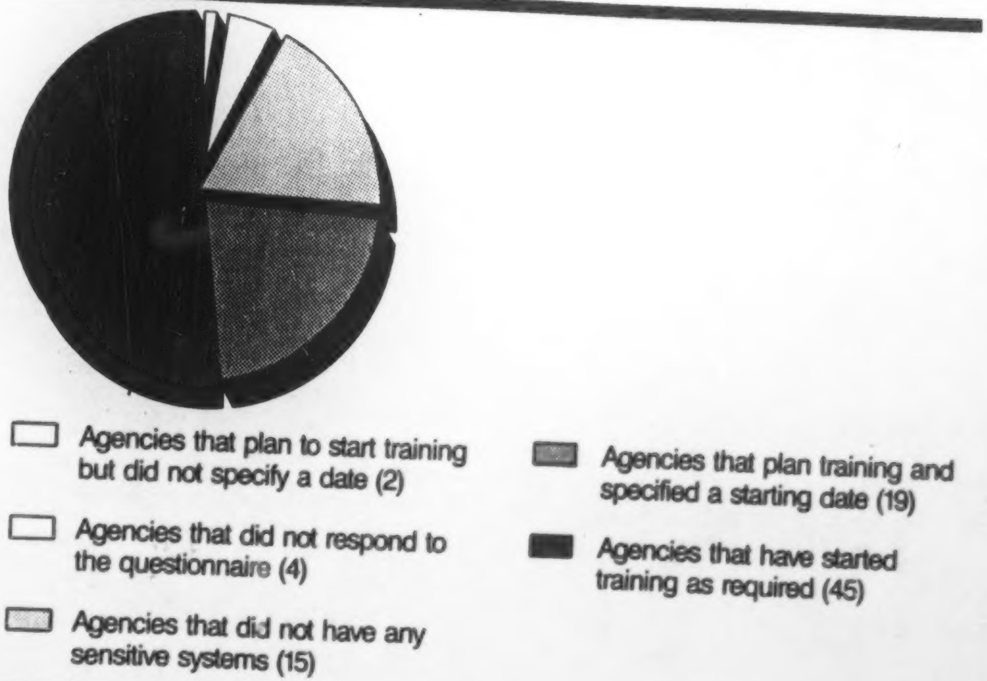

CHART 2

GAO

Compliance with Security Plan Requirements, as of March 6, 1989

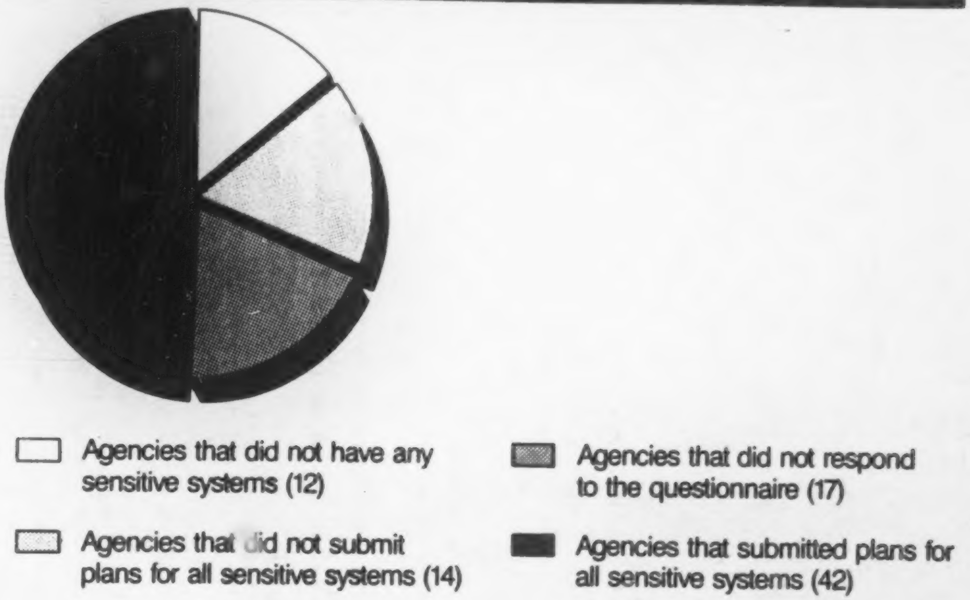

CHART 3

Sensitive Systems Operated by Other Organizations as Reported by the Ten Agencies

	Systems operated by	
Departments	Contractor	State or local government
Agriculture[1]	9	0
Defense[2]	35	0
Energy[3]	-	-
Health and Human Services[4]	31	0
Interior[5]	4	0
Justice	4	0
Labor	4	0
Treasury[6]	5	0
Other		
Environmental Protection Agency	0	0
National Aeronautics and Space Administration[7]	29	0
Totals	121	0

---

[1] Department of Agriculture's response did not include information from all of its agencies.

[2] Department of Defense's response did not include information on the Air Force, Army, or Navy. The Department said the remaining information would be available in 90 days.

[3] Department of Energy's response did not include information on its systems. The Department said it requested its components to certify that they had identified all of their sensitive systems.

[4] One of the systems reported by the Department of Health and Human Services is operated by contractors at 88 different locations.

[5] Department of the Interior incorrectly reported three sensitive systems. The Department's response omitted the White House Inventory and Museum System.

[6] Department of the Treasury's response did not show the operators of the systems. The Department provided system and operator information to GAO on February 6, 1989, however, a system operated by the Federal Reserve Board was omitted from the list.

[7] National Aeronautics and Space Administration prepared a list of 29 systems but inadvertently submitted to the Committees a response containing 15 systems.

Mr. Walgren. All right. Thank you.

Mr. Gill, do you want to add anything to that presentation?

[No response.]

Mr. Walgren. I guess I'd like to ask Mr. McDonough, as I understand it, GSA has submitted their security plans to NIST and to NSA for comment.

Is there anything that can be concluded from that experience that perhaps would be helpful to OMB and to others about the problems and the value of that kind of interaction?

Mr. McDonough. As the Admiral said, the lessons are coming in and will be studied in the weeks ahead. One I know I would suggest perhaps for OPM would be that I think some of the early feedback from this says that we ought to be sure that we're training all levels of people that would be exposed to the computer security issue. And that means down at the user level—program managers, and it means senior executives.

It might be useful for OPM to develop a model of training that would be appropriate for each of those levels. It might be worth consideration rather than having every agency try to identify that kind of a model for themselves.

Mr. Walgren. Now, in your testimony, you indicate that GSA has awarded, as I understand it, a single nationwide contract for computer security services.

Mr. McDonough. Yes, we did.

Mr. Walgren. That must be a pretty expensive contract. Is it natural for that to go to one entity?

Mr. McDonough. I think so considering the level of activity that we expect under it. Perhaps something on the order of $3 million a year, maybe about 20 task orders per year. We wouldn't want to fragment it below that. That seems to be a good number for the business we expect under it, Mr. Chairman.

Mr. Walgren. Can the kind of work that needs to be done be done for several million dollars a year?

Mr. McDonough. I think so. We'll have to watch that. Obviously, if the business grows—in other words, we have in the government about 20 major agencies and about 45 quite small ones, and commissions in there. And we're going to need to think through the methodology and how they're going to conduct this business in the years ahead.

Having done that, once they have the model, it may not be the kind of thing that needs to be repeated. It's on that basis that we arrived at that projected size.

Mr. Walgren. In the process of that, you're going to develop an electronic bulletin board that will be available to client agencies of GSA, but not available to anybody else.

Would that not be useful for others as well? Does it make sense to have a general electronic bulletin board that all interested agencies could learn from?

Mr. McDonough. It could. This particular bulletin board will contain information on it that GSA thinks is needed. It will also contain information that is relative to the services of this contractor and so the bulletin board will cost money, and we anticipate that it will be funded—the overhead by the clients of the contractor.

We had not planned to make it available on an access basis to other agencies. That would require a fairly difficult billing system. But it's the kind of thing that we can watch. There's a tremendous demand there, other alternatives could be considered.

Mr. **Walgren**. Let me ask you, Mr. Rhile, what your instinct is for the rate of compliance with undertaking training and development plans under this Act.

Mr. **Rhile**. As you know, Mr. Chairman, we've done three questionnaires, one on the identification of sensitive systems, one on training and one on security plans.

I think, based on looking back across that work, I would have to say that it looks like there's an impressive amount of agency activity toward complying with this Act. As compared to a year ago, agencies have identified their sensitive systems and put training programs in place. Most of the rest are planning to do so shortly.

Mr. **Walgren**. Do you have good confidence that those who say they have no sensitive systems have no sensitive systems?

Mr. **Rhile**. I heard that question asked before today and I don't have the list with me. I can provide it for the record. But most of those agencies are smaller agencies, such as the American Battlefield Monuments Commission. And some of them I don't think reported any computer systems at all.

So it is quite possible that some of those smaller ones would not have sensitive systems. I can provide an analysis of that for the record.

Two of them, of course, are the National Security Council and the CIA, which reported to us that their systems are protected in accordance with the regulations concerning classified information.

[The material referred to follows:]

GAO
United States
General Accounting Office
Washington, D.C. 20548

Information Management and
Technology Division

April 21, 1989

APR 27 1989

The Honorable Tim Valentine
Chairman, Subcommittee on Transportation,
  Aviation, and Materials,
Committee on Science, Space, and Technology
House of Representatives

The Honorable Doug Walgren
Chairman, Subcommittee on Science, Research,
  and Technology,
Committee on Science, Space, and Technology
House of Representatives

Dear Chairmen:

During our testimony at the March 21, 1989, hearings on the Computer Security Act of 1987, we agreed to provide for the record some additional information about the 12 federal agencies that reported that they do not have any sensitive computer systems, as defined by the act. Since the hearings, five other agencies have also reported that they do not have any sensitive computer systems. As agreed with your offices, we did not independently verify the agencies' responses. Attachment I summarizes the responses provided by the 17 agencies.

Should you have any questions concerning this letter, please contact Howard Rhile, Associate Director, on 275-9675.

Sincerely,

Daniel C. White
for Ralph V. Carlone
Assistant Comptroller General

Enclosure

Administrative Conference of the U.S.

The Conference said it has one computer system that is used to maintain mailing lists and budget information. According to the Conference, the system does not process sensitive information.

Advisory Council on Historic Preservation

The Council reported that administrative services such as accounting, payroll, personnel, and procurement are provided by the Department of the Interior. The Council said it has ten personal computers that it will use for word processing and data base support. The Council reported that none of the information processed on the personal computers is sensitive.

African Development Foundation

The Foundation said it has one computer system, which is used for office support. The Foundation stated that this computer system does not process sensitive information.

American Battle Monuments Commission

The Commission reported that it has five computer systems. According to the Commission, these systems do not process sensitive information.

Central Intelligence Agency

As we reported in our December 8, 1988, letter to the Chairman, Subcommittee on Transportation, Aviation, and Materials, Committee on Science, Space, and Technology, the CIA indicated that its computer systems are exempt from the Computer Security Act of 1987 based on 44 U.S.C. Section 3502(2). According to a CIA legislative attorney, all of its computer systems contain at least some classified or intelligence information and therefore are subject to stricter security requirements than those in the act.

Commission on the Bicentennial of the U.S. Constitution

The Commission initially stated that it had one computer system, which processes sensitive information. The Commission later reported that it has two computer systems which do not process sensitive information.

Commission of Fine Arts

The Commission reported that it does not have any computer systems.

Commission on Civil Rights

The Commission initially reported that it had five computer systems, of which four process sensitive information. The Commission later stated that it has no systems, which process sensitive information.

Committee for Purchase from the Blind and Other Severely Handicapped

The Committee said it has one computer system, which does not process sensitive information.

Federal Mediation and Conciliation Service

The Service stated that it has two computer systems, which do not process sensitive information. According to the Service, it receives payroll and personnel support from the Securities and Exchange Commission, which has reported on the computer systems.

Foreign Claims Settlement Commission of the U.S.

The Commission reported that it has three computer systems, which do not process sensitive information.

Joint Financial Management Improvement Program

The Program said it does not have any computer systems that process sensitive information.

National Commission on Libraries and Information

The Commission reported that it has one computer system, which does not process sensitive information.

National Security Council

The Council reported that all computer systems operated by or on behalf of the Council are protected at least at the top-secret level.

National Transportation Safety Board

The Board reported that it has 26 computer systems, which do not process sensitive information.

Postal Rate Commission

The Commission reported that it has seven computer systems, which do not process sensitive information.

Smithsonian Institution

The Institution reported that the Computer Security Act of 1987 does not apply to it because it does not operate federal computer systems and its systems do not process sensitive information.

Mr. WALGREN. They do not call for...I see. So that they do not fall...

Mr. RHILE. They do not fall under the purview for that reason.

Mr. WALGREN. Classified.

Mr. RHILE. Yes. However, the CIA, were it to have sensitive information as defined by the Act, would, indeed, be under the purview of the Act.

Mr. WALGREN. It would seem unusual that they do not have sensitive information, but it may be—I guess I don't know how this works. If an agency has both sensitive information and classified information, can they maintain the sensitive the same?

Mr. RHILE. We did a little research on that as a result of last September's hearing. What they're telling us is that their systems contain at least some classified information in each system. Therefore, they are protecting it as classified as opposed to protecting the system as just containing, quote, "just sensitive information."

Mr. WALGREN. I see. We'd appreciate that list that you mentioned of those who have reported no sensitive information.

What's the impression of the reports that those who are just coming in now who have not responded to the survey but, as you say, in the last week, a number, nine of the 17 have now reported.

What's the characterization of their report? Is it an adequate report? Or is it something that was just filed in order to have a piece of paper on file?

Mr. RHILE. We received some of those. I guess we received one yesterday and a couple before. What we are referring to are responses to our questionnaire that was sent out in January and February on the security plans.

I think one of them said that it was lost in the mail or something like that. And they had to resubmit it.

But I haven't really had an opportunity to go over them in any kind of detail.

Mr. WALGREN. I don't know the depth of your inquiry. Is it possible to tell whether there is a substantive response, a substantive plan, in these agencies versus something which might not be characterized as a serious response or a serious compliance?

Mr. RHILE. What we are asking the agencies in our questionnaire are:

Do you have security plans? Have you submitted them in accordance with the Act? If not, why not? How many plans have you submitted? How many systems are covered by those plans? Who are these systems operated by? Yourself? Contractors? States, and so forth. Are you satisfied with the regulations and the OPM guidance, and so forth and so on.

We did not ask for copies of the plans themselves to do an independent evaluation of the plans. Our objective, as we discussed with the Committee, was to determine whether they were in compliance with the Act on the basis of their response to our questionnaire. I can say that the agencies who have responded recently have filled out the questionnaire.

In fact, we've been in contact with them over the last couple of weeks. So I have no reason to believe that the response is perfunctory or otherwise not sincere.

Mr. Walgren. All right. On behalf of the Committee, we appreciate your coming and being a contact and a resource for us. And we plan to talk to you again about this area.

Thank you very much.

[Whereupon, at 4:30 p.m., the Subcommittee was adjourned.]

○

BEST AVAILABLE COPY